

<http://buildings.honeywell.com/security>

The purpose of this document is to identify the patches that have been delivered by Microsoft® which have been tested against Pro-Watch. All the below listed patches have been tested against the current shipping version of Pro-Watch with no adverse effects being observed. Microsoft Patches were evaluated up to and including [CVE-2024-49043/ CVE-2024-7005](#), patches not listed below are not applicable to a Pro-Watch system.

## 2024 – Microsoft® Patches Tested with Pro-Watch

### Nov 2024:

<a href="#">CVE-2024-49043</a>	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability
<a href="#">CVE-2024-49039</a>	Windows Task Scheduler Elevation of Privilege Vulnerability
<a href="#">CVE-2024-49021</a>	Microsoft SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-49019</a>	Active Directory Certificate Services Elevation of Privilege Vulnerability
<a href="#">CVE-2024-49018</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49017</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49016</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49015</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49014</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49013</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49012</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49011</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49010</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49009</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49008</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49007</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49006</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49005</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49004</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49003</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49002</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49001</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-49000</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48999</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48998</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48997</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48996</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48995</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48994</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-48993</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-43644</a>	Windows Client-Side Caching Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43642</a>	Windows SMB Denial of Service Vulnerability
<a href="#">CVE-2024-43641</a>	Windows Registry Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43640</a>	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43639</a>	Windows KDC Proxy Remote Code Execution Vulnerability
<a href="#">CVE-2024-43636</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43635</a>	Windows Telephony Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-43630</a>	Windows Kernel Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-43629</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43626</a>	Windows Telephony Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43622</a>	Windows Telephony Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-43462</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-43462</a>	SQL Server Native Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-43451</a>	NTLM Hash Disclosure Spoofing Vulnerability
<a href="#">CVE-2024-38203</a>	Windows Package Library Manager Information Disclosure Vulnerability

## **Oct 2024:**

<a href="#">CVE-2024-43611</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43607</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43599</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-43593</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43592</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43589</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43585</a>	Code Integrity Guard Security Feature Bypass Vulnerability
<a href="#">CVE-2024-43584</a>	Windows Scripting Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2024-43583</a>	Winlogon Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43582</a>	Remote Desktop Protocol Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-43575</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-43574</a>	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43573</a>	Windows MSHTML Platform Spoofing Vulnerability
<a href="#">CVE-2024-43572</a>	Microsoft Management Console Remote Code Execution Vulnerability
<a href="#">CVE-2024-43570</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43562</a>	Windows Network Address Translation (NAT) Denial of Service Vulnerability
<a href="#">CVE-2024-43558</a>	Windows Mobile Broadband Driver Denial of Service Vulnerability
<a href="#">CVE-2024-43553</a>	NT OS Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43549</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-43540</a>	Windows Mobile Broadband Driver Denial of Service Vulnerability
<a href="#">CVE-2024-43536</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-43534</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2024-43526</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-43518</a>	Windows Telephony Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-43511</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-43506</a>	BranchCache Denial of Service Vulnerability
<a href="#">CVE-2024-43484</a>	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability
<a href="#">CVE-2024-43483</a>	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability
<a href="#">CVE-2024-37983</a>	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability

## **Sep 2024:**

<a href="#">CVE-2024-43487</a>	Windows Mark of the Web Security Feature Bypass Vulnerability
<a href="#">CVE-2024-43461</a>	Windows MSHTML Platform Spoofing Vulnerability
<a href="#">CVE-2024-43458</a>	Windows Networking Information Disclosure Vulnerability
<a href="#">CVE-2024-43455</a>	Windows Remote Desktop Licensing Service Spoofing Vulnerability
<a href="#">CVE-2024-43454</a>	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38263</a>	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38260</a>	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-38259</a>	Microsoft Management Console Remote Code Execution Vulnerability
<a href="#">CVE-2024-38258</a>	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability
<a href="#">CVE-2024-38257</a>	Microsoft AIJoyn API Information Disclosure Vulnerability
<a href="#">CVE-2024-38249</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38248</a>	Windows Storage Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38247</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38246</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38245</a>	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38244</a>	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38243</a>	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38239</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38237</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38235</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-38119</a>	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability
<a href="#">CVE-2024-38045</a>	Windows TCP/IP Remote Code Execution Vulnerability
<a href="#">CVE-2024-38014</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2024-37980</a>	Microsoft SQL Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-37966</a>	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
<a href="#">CVE-2024-37965</a>	Microsoft SQL Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-37342</a>	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
<a href="#">CVE-2024-37341</a>	Microsoft SQL Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-37340</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-37339</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-37338</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-37337</a>	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
<a href="#">CVE-2024-37335</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-30073</a>	Windows Security Zone Mapping Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26191</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-26186</a>	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
<a href="#">CVE-2024-21416</a>	Windows TCP/IP Remote Code Execution Vulnerability

## **Aug 2024:**

<a href="#">CVE-2024-38223</a>	Windows Initial Machine Configuration Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38215</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38214</a>	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
<a href="#">CVE-2024-38199</a>	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38193</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38180</a>	Windows SmartScreen Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38178</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2024-38155</a>	Security Center Broker Information Disclosure Vulnerability
<a href="#">CVE-2024-38154</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-38153</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38152</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2024-38151</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2024-38150</a>	Windows DWM Core Library Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-38148</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2024-38147</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38146</a>	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
<a href="#">CVE-2024-38143</a>	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38140</a>	Windows Reliable Multicast Transport Driver (RMCST) Remote Code Execution Vulnerability
<a href="#">CVE-2024-38134</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38127</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38122</a>	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability
<a href="#">CVE-2024-38120</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-38117</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38106</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-37968</a>	Windows DNS Spoofing Vulnerability
<a href="#">CVE-2022-3775</a>	Redhat: CVE-2022-3775 grub2 - Heap based out-of-bounds write when rendering certain Unicode se

## **July 2024:**

<a href="#">CVE-2024-39379</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2024-38176</a>	GroupMe Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38164</a>	GroupMe Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38156</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2024-38103</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-38099</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38095</a>	.NET and Visual Studio Denial of Service Vulnerability
<a href="#">CVE-2024-38081</a>	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38081</a>	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38081</a>	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38073</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38070</a>	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38069</a>	Windows Enroll Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38069</a>	Windows Enroll Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38068</a>	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
<a href="#">CVE-2024-38066</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38065</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38058</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38057</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38057</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38053</a>	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-38049</a>	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability
<a href="#">CVE-2024-38047</a>	PowerShell Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38047</a>	PowerShell Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38044</a>	DHCP Server Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38030</a>	Windows Themes Spoofing Vulnerability
<a href="#">CVE-2024-38027</a>	Windows Line Printer Daemon Service Denial of Service Vulnerability
<a href="#">CVE-2024-38017</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2024-38011</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38011</a>	Secure Boot Security Feature Bypass Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-38010</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37989</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37989</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37988</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37984</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37334</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-30105</a>	.NET Core and Visual Studio Denial of Service Vulnerability
<a href="#">CVE-2024-7005</a>	Chromium: CVE-2024-7005 Insufficient validation of untrusted input in Safe Browsing
<a href="#">CVE-2024-7004</a>	Chromium: CVE-2024-7004 Insufficient validation of untrusted input in Safe Browsing
<a href="#">CVE-2024-7003</a>	Chromium: CVE-2024-7003 Inappropriate implementation in FedCM
<a href="#">CVE-2024-7001</a>	Chromium: CVE-2024-7001 Inappropriate implementation in HTML
<a href="#">CVE-2024-7000</a>	Chromium: CVE-2024-7000 Use after free in CSS
<a href="#">CVE-2024-6999</a>	Chromium: CVE-2024-6999 Inappropriate implementation in FedCM
<a href="#">CVE-2024-6998</a>	Chromium: CVE-2024-6998 Use after free in User Education
<a href="#">CVE-2024-6997</a>	Chromium: CVE-2024-6997 Use after free in Tabs
<a href="#">CVE-2024-6996</a>	Chromium: CVE-2024-6996 Race in Frames
<a href="#">CVE-2024-6995</a>	Chromium: CVE-2024-6995 Inappropriate implementation in Fullscreen
<a href="#">CVE-2024-6994</a>	Chromium: CVE-2024-6994 Heap buffer overflow in Layout
<a href="#">CVE-2024-6993</a>	Chromium: CVE-2024-6993
<a href="#">CVE-2024-6992</a>	Chromium: CVE-2024-6992
<a href="#">CVE-2024-6991</a>	Chromium: CVE-2024-6991 Use after free in Dawn
<a href="#">CVE-2024-6989</a>	Chromium: CVE-2024-6989 Use after free in Loader
<a href="#">CVE-2024-6988</a>	Chromium: CVE-2024-6988 Use after free in Downloads
<a href="#">CVE-2024-6779</a>	Chromium: CVE-2024-6779 Out of bounds memory access in V8
<a href="#">CVE-2024-6778</a>	Chromium: CVE-2024-6778 Race in DevTools
<a href="#">CVE-2024-6777</a>	Chromium: CVE-2024-6777 Use after free in Navigation
<a href="#">CVE-2024-6776</a>	Chromium: CVE-2024-6776 Use after free in Audio
<a href="#">CVE-2024-6775</a>	Chromium: CVE-2024-6775 Use after free in Media Stream
<a href="#">CVE-2024-6774</a>	Chromium: CVE-2024-6774 Use after free in Screen Capture
<a href="#">CVE-2024-6773</a>	Chromium: CVE-2024-6773 Type Confusion in V8
<a href="#">CVE-2024-6772</a>	Chromium: CVE-2024-6772 Inappropriate implementation in V8
<a href="#">CVE-2024-6387</a>	RedHat Openssh: CVE-2024-6387 Remote Code Execution Due To A Race Condition In Signal Handling

## **June 2024:**

<a href="#">CVE-2024-39684</a>	Github: CVE-2024-39684 TenCent RapidJSON Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38105</a>	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
<a href="#">CVE-2024-38101</a>	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
<a href="#">CVE-2024-38099</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38079</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38078</a>	Xbox Wireless Adapter Remote Code Execution Vulnerability
<a href="#">CVE-2024-38076</a>	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38073</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38070</a>	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38069</a>	Windows Enroll Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38068</a>	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-38066</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38065</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38058</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38057</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38053</a>	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-38052</a>	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38050</a>	Windows Workstation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38049</a>	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability
<a href="#">CVE-2024-38047</a>	PowerShell Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38044</a>	DHCP Server Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38033</a>	PowerShell Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38032</a>	Microsoft Xbox Remote Code Execution Vulnerability
<a href="#">CVE-2024-38030</a>	Windows Themes Spoofing Vulnerability
<a href="#">CVE-2024-38028</a>	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability
<a href="#">CVE-2024-38027</a>	Windows Line Printer Daemon Service Denial of Service Vulnerability
<a href="#">CVE-2024-38017</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2024-38011</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38010</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37989</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37988</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-37984</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-39684</a>	Github: CVE-2024-39684 TenCent RapidJSON Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38105</a>	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
<a href="#">CVE-2024-38101</a>	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
<a href="#">CVE-2024-38099</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38079</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2024-38078</a>	Xbox Wireless Adapter Remote Code Execution Vulnerability
<a href="#">CVE-2024-38076</a>	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-38073</a>	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
<a href="#">CVE-2024-38070</a>	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-38069</a>	Windows Enroll Engine Security Feature Bypass Vulnerability

## **May 2024:**

<a href="#">CVE-2024-30051</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30050</a>	Windows Mark of the Web Security Feature Bypass Vulnerability
<a href="#">CVE-2024-30049</a>	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30040</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2024-30039</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-30038</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30037</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30036</a>	Windows Deployment Services Information Disclosure Vulnerability
<a href="#">CVE-2024-30035</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30034</a>	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2024-30033</a>	Windows Search Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30032</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30031</a>	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-30029</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30028</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30027</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30025</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30024</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30023</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30022</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30021</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30020</a>	Windows Cryptographic Services Remote Code Execution Vulnerability
<a href="#">CVE-2024-30019</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2024-30018</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-30017</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2024-30016</a>	Windows Cryptographic Services Information Disclosure Vulnerability
<a href="#">CVE-2024-30015</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30014</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30012</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30011</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-30010</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2024-30009</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-30008</a>	Windows DWM Core Library Information Disclosure Vulnerability
<a href="#">CVE-2024-30006</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-30005</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30004</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30003</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30002</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30001</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-30000</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-29999</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-29998</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-29997</a>	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-29996</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-29994</a>	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability
<a href="#">CVE-2024-29984</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-29983</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-29046</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-29045</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-29044</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28945</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28944</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28943</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28941</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28940</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28939</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28938</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28937</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-28935</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28934</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28933</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28931</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28930</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28929</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28927</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28926</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28915</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28914</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28913</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28911</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28910</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28906</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26238</a>	Microsoft PLUGScheduler Scheduled Task Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21409</a>	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2024-5274</a>	Chromium CVE-2024-5274 Type Confusion in V8
<a href="#">CVE-2024-5160</a>	Chromium CVE-2024-5160 Heap buffer overflow in Dawn
<a href="#">CVE-2024-5159</a>	Chromium CVE-2024-5159 Heap buffer overflow in ANGLE
<a href="#">CVE-2024-5158</a>	Chromium CVE-2024-5158 Type Confusion in V8
<a href="#">CVE-2024-5157</a>	Chromium CVE-2024-5157 Use after free in Scheduling
<a href="#">CVE-2024-4950</a>	Chromium CVE-2024-4950 Inappropriate implementation in Downloads
<a href="#">CVE-2024-4949</a>	Chromium CVE-2024-4949 Use after free in V8
<a href="#">CVE-2024-4948</a>	Chromium CVE-2024-4948 Use after free in Dawn
<a href="#">CVE-2024-4947</a>	Chromium CVE-2024-4947 Type Confusion in V8
<a href="#">CVE-2024-4761</a>	Chromium CVE-2024-4761 Out of bounds write in V8
<a href="#">CVE-2024-4671</a>	Chromium CVE-2024-4671 Use after free in Visuals
<a href="#">CVE-2024-4559</a>	Chromium CVE-2024-4559 Heap buffer overflow in WebAudio
<a href="#">CVE-2024-4558</a>	Chromium CVE-2024-4558 Use after free in ANGLE
<a href="#">CVE-2024-4368</a>	Chromium CVE-2024-4368 Use after free in Dawn
<a href="#">CVE-2024-4331</a>	Chromium CVE-2024-4331 Use after free in Picture In Picture
<a href="#">CVE-2024-30056</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-30055</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability

## **April 2024:**

<a href="#">CVE-2024-29988</a>	SmartScreen Prompt Security Feature Bypass Vulnerability
<a href="#">CVE-2024-29066</a>	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-29064</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-29062</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-29061</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-29056</a>	Windows Authentication Elevation of Privilege Vulnerability
<a href="#">CVE-2024-29052</a>	Windows Storage Elevation of Privilege Vulnerability
<a href="#">CVE-2024-29050</a>	Windows Cryptographic Services Remote Code Execution Vulnerability
<a href="#">CVE-2024-29044</a>	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-29043</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-28943</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28941</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28938</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28937</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28936</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28935</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28934</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28933</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28932</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28931</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28930</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28929</a>	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-28925</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28924</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28923</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28922</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28921</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28920</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28919</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28903</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28902</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-28901</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-28900</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-28898</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28897</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-28896</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26255</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-26254</a>	Microsoft Virtual Machine Bus (VMBus) Denial of Service Vulnerability
<a href="#">CVE-2024-26253</a>	sys Remote Code Execution Vulnerability
<a href="#">CVE-2024-26252</a>	Windows rndismp6.sys Remote Code Execution Vulnerability
<a href="#">CVE-2024-26252</a>	sys Remote Code Execution Vulnerability
<a href="#">CVE-2024-26250</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26248</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26244</a>	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26243</a>	Windows USB Print Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26242</a>	Windows Telephony Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26241</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26240</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26239</a>	Windows Telephony Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26237</a>	Windows Defender Credential Guard Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26234</a>	Proxy Driver Spoofing Vulnerability
<a href="#">CVE-2024-26233</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26232</a>	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability
<a href="#">CVE-2024-26231</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26230</a>	Windows Telephony Server Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-26229</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26228</a>	Windows Cryptographic Services Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26227</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26226</a>	Windows Distributed File System (DFS) Information Disclosure Vulnerability
<a href="#">CVE-2024-26224</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26223</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26222</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26221</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26220</a>	Windows Mobile Hotspot Information Disclosure Vulnerability
<a href="#">CVE-2024-26219</a>	sys Denial of Service Vulnerability
<a href="#">CVE-2024-26218</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26217</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-26216</a>	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26215</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2024-26214</a>	Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-26212</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2024-26211</a>	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26210</a>	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26209</a>	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
<a href="#">CVE-2024-26208</a>	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability
<a href="#">CVE-2024-26207</a>	Windows Remote Access Connection Manager Information Disclosure Vulnerability
<a href="#">CVE-2024-26205</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-26202</a>	DHCP Server Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-26200</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-26195</a>	DHCP Server Service Remote Code Execution Vulnerability
<a href="#">CVE-2024-26194</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26189</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26183</a>	Windows Kerberos Denial of Service Vulnerability
<a href="#">CVE-2024-26180</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26179</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2024-26175</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26172</a>	Windows DWM Core Library Information Disclosure Vulnerability
<a href="#">CVE-2024-26171</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26168</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26158</a>	Microsoft Install Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-23594</a>	Stack buffer overflow in Lenovo system recovery boot manager
<a href="#">CVE-2024-23593</a>	Zero Out Boot Manager and drop to UEFI Shell
<a href="#">CVE-2024-23593</a>	Lenovo: CVE-2024-23593 Zero Out Boot Manager and drop to UEFI Shell
<a href="#">CVE-2024-21447</a>	Windows Authentication Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21409</a>	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2024-21409</a>	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2024-20693</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20689</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-20688</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-20678</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-20669</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2024-20665</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2022-0001</a>	Branch History Injection
<a href="#">CVE-2022-0001</a>	Intel: CVE-2022-0001 Branch History Injection
<a href="#">CVE-2024-29049</a>	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability
<a href="#">CVE-2024-29981</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2024-29986</a>	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-29987</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-29991</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-3156</a>	Chromium CVE-2024-3156 Inappropriate implementation in V8
<a href="#">CVE-2024-3157</a>	Chromium CVE-2024-3157 Out of bounds write in Compositing
<a href="#">CVE-2024-3158</a>	Chromium CVE-2024-3158 Use after free in Bookmarks
<a href="#">CVE-2024-3159</a>	Chromium CVE-2024-3159 Out of bounds memory access in V8
<a href="#">CVE-2024-3515</a>	Chromium CVE-2024-3515 Use after free in Dawn
<a href="#">CVE-2024-3516</a>	Chromium CVE-2024-3516 Heap buffer overflow in ANGLE
<a href="#">CVE-2024-3832</a>	Chromium CVE-2024-3832 Object corruption in V8
<a href="#">CVE-2024-3833</a>	Chromium CVE-2024-3833 Object corruption in WebAssembly
<a href="#">CVE-2024-3834</a>	Chromium CVE-2024-3834 Use after free in Downloads
<a href="#">CVE-2024-3837</a>	Chromium CVE-2024-3837 Use after free in QUIC
<a href="#">CVE-2024-3838</a>	Chromium CVE-2024-3838 Inappropriate implementation in Autofill
<a href="#">CVE-2024-3839</a>	Chromium CVE-2024-3839 Out of bounds read in Fonts
<a href="#">CVE-2024-3840</a>	Chromium CVE-2024-3840 Insufficient policy enforcement in Site Isolation
<a href="#">CVE-2024-3841</a>	Chromium CVE-2024-3841 Insufficient data validation in Browser Switcher
<a href="#">CVE-2024-3843</a>	Chromium CVE-2024-3843 Insufficient data validation in Downloads
<a href="#">CVE-2024-3844</a>	Chromium CVE-2024-3844 Inappropriate implementation in Extensions
<a href="#">CVE-2024-3845</a>	Chromium CVE-2024-3845 Inappropriate implementation in Network
<a href="#">CVE-2024-3846</a>	Chromium CVE-2024-3846 Inappropriate implementation in Prompts
<a href="#">CVE-2024-3847</a>	Chromium CVE-2024-3847 Insufficient policy enforcement in WebUI
<a href="#">CVE-2024-3914</a>	Chromium CVE-2024-3914 Use after free in V8

## **March 2024:**

<a href="#">CVE-2024-26197</a>	Windows Standards-Based Storage Management Service Denial of Service Vulnerability
<a href="#">CVE-2024-26190</a>	Microsoft QUIC Denial of Service Vulnerability
<a href="#">CVE-2024-26182</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26181</a>	Windows Kernel Denial of Service Vulnerability
<a href="#">CVE-2024-26178</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26177</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2024-26176</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26174</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2024-26173</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26170</a>	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26169</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2024-26166</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26162</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-26161</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-26160</a>	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2024-26159</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-21451</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-21450</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-21446</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21445</a>	Windows USB Print Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21444</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-21443</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21442</a>	Windows USB Print Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21441</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2024-21440</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-21439</a>	Windows Telephony Server Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21438</a>	Microsoft AllJoyn API Denial of Service Vulnerability
<a href="#">CVE-2024-21437</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21436</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21434</a>	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21433</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21432</a>	Windows Update Stack Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21431</a>	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-21430</a>	Windows USB Attached SCSI (UAS) Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2024-21429</a>	Windows USB Hub Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-21427</a>	Windows Kerberos Security Feature Bypass Vulnerability
<a href="#">CVE-2024-21408</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-21407</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2023-28746</a>	Register File Data Sampling (RFDS)
<a href="#">CVE-2024-29057</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2024-2887</a>	Chromium CVE-2024-2887 Type Confusion in WebAssembly
<a href="#">CVE-2024-2886</a>	Chromium CVE-2024-2886 Use after free in WebCodecs
<a href="#">CVE-2024-2885</a>	Chromium CVE-2024-2885 Use after free in Dawn
<a href="#">CVE-2024-2883</a>	Chromium CVE-2024-2883 Use after free in ANGLE
<a href="#">CVE-2024-2631</a>	Chromium CVE-2024-2631 Inappropriate implementation in iOS
<a href="#">CVE-2024-2630</a>	Chromium CVE-2024-2630 Inappropriate implementation in iOS
<a href="#">CVE-2024-2629</a>	Chromium CVE-2024-2629 Incorrect security UI in iOS
<a href="#">CVE-2024-2628</a>	Chromium CVE-2024-2628 Inappropriate implementation in Downloads
<a href="#">CVE-2024-2627</a>	Chromium CVE-2024-2627 Use after free in Canvas
<a href="#">CVE-2024-2626</a>	Chromium CVE-2024-2626 Out of bounds read in Swiftshader
<a href="#">CVE-2024-2625</a>	Chromium CVE-2024-2625 Object lifecycle issue in V8
<a href="#">CVE-2024-26247</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-26163</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-2400</a>	Chromium CVE-2024-2400 Use after free in Performance Manager
<a href="#">CVE-2024-2176</a>	Chromium CVE-2024-2176 Use after free in FedCM
<a href="#">CVE-2024-2174</a>	Chromium CVE-2024-2174 Inappropriate implementation in V8
<a href="#">CVE-2024-2173</a>	Chromium CVE-2024-2173 Out of bounds memory access in V8
<a href="#">CVE-2024-1939</a>	Chromium CVE-2024-1939 Type Confusion in V8

<http://buildings.honeywell.com/security>

[CVE-2024-1938](#) Chromium CVE-2024-1938 Type Confusion in V8

## **February 2024:**

[CVE-2024-21420](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21412](#) Internet Shortcut Files Security Feature Bypass Vulnerability  
[CVE-2024-21406](#) Windows Printing Service Spoofing Vulnerability  
[CVE-2024-21405](#) Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability  
[CVE-2024-21391](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21377](#) Windows DNS Information Disclosure Vulnerability  
[CVE-2024-21375](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21372](#) Windows OLE Remote Code Execution Vulnerability  
[CVE-2024-21371](#) Windows Kernel Elevation of Privilege Vulnerability  
[CVE-2024-21370](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21369](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21368](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21367](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21366](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21365](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21363](#) Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability  
[CVE-2024-21362](#) Windows Kernel Security Feature Bypass Vulnerability  
[CVE-2024-21362](#) Windows Kernel Security Feature Bypass Vulnerability  
[CVE-2024-21361](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21360](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21359](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21358](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21357](#) Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability  
[CVE-2024-21356](#) Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability  
[CVE-2024-21355](#) Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability  
[CVE-2024-21352](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21351](#) Windows SmartScreen Security Feature Bypass Vulnerability  
[CVE-2024-21350](#) Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability  
[CVE-2024-21349](#) Microsoft ActiveX Data Objects Remote Code Execution Vulnerability  
[CVE-2024-21348](#) Internet Connection Sharing (ICS) Denial of Service Vulnerability  
[CVE-2024-21347](#) Microsoft ODBC Driver Remote Code Execution Vulnerability  
[CVE-2024-21346](#) Win32k Elevation of Privilege Vulnerability  
[CVE-2024-21344](#) Windows Network Address Translation (NAT) Denial of Service Vulnerability  
[CVE-2024-21343](#) Windows Network Address Translation (NAT) Denial of Service Vulnerability  
[CVE-2024-21342](#) Windows DNS Client Denial of Service Vulnerability  
[CVE-2024-21341](#) Windows Kernel Remote Code Execution Vulnerability  
[CVE-2024-21340](#) Windows Kernel Information Disclosure Vulnerability  
[CVE-2024-21339](#) Windows USB Generic Parent Driver Remote Code Execution Vulnerability  
[CVE-2024-21339](#) Windows USB Generic Parent Driver Remote Code Execution Vulnerability  
[CVE-2024-21338](#) Windows Kernel Elevation of Privilege Vulnerability  
[CVE-2024-21304](#) Trusted Compute Base Elevation of Privilege Vulnerability  
[CVE-2024-20684](#) Windows Hyper-V Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-50387</a>	NSSEC verification complexity can be exploited to exhaust CPU resources and stall DNS resolvers MITRE: CVE-2023-50387 DNSSEC verification complexity can be exploited to exhaust CPU resources
<a href="#">CVE-2023-50387</a>	DNS resolvers
<a href="#">CVE-2024-26192</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-21423</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2024-21399</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2024-1676</a>	Chromium CVE-2024-1676 Inappropriate implementation in Navigation
<a href="#">CVE-2024-1675</a>	Chromium CVE-2024-1675 Insufficient policy enforcement in Download
<a href="#">CVE-2024-1674</a>	Chromium CVE-2024-1674 Inappropriate implementation in Navigation
<a href="#">CVE-2024-1673</a>	Chromium CVE-2024-1673 Use after free in Accessibility
<a href="#">CVE-2024-1672</a>	Chromium CVE-2024-1672 Inappropriate implementation in Content Security Policy
<a href="#">CVE-2024-1671</a>	Chromium CVE-2024-1671 Inappropriate implementation in Site Isolation
<a href="#">CVE-2024-1670</a>	Chromium CVE-2024-1670 Use after free in Mojo
<a href="#">CVE-2024-1669</a>	Chromium CVE-2024-1669 Out of bounds memory access in Blink
<a href="#">CVE-2024-1284</a>	Chromium CVE-2024-1284 Use after free in Mojo
<a href="#">CVE-2024-1283</a>	Chromium CVE-2024-1283 Heap buffer overflow in Skia
<a href="#">CVE-2024-1077</a>	Chromium CVE-2024-1077 Use after free in Network
<a href="#">CVE-2024-1060</a>	Chromium CVE-2024-1060 Use after free in Canvas

## **January 2024:**

<a href="#">CVE-2024-21320</a>	Windows Themes Spoofing Vulnerability
<a href="#">CVE-2024-21316</a>	No Vulnerability Name Found
<a href="#">CVE-2024-21314</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2024-21313</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2024-21312</a>	NET Framework Denial of Service Vulnerability
<a href="#">CVE-2024-21311</a>	Windows Cryptographic Services Information Disclosure Vulnerability
<a href="#">CVE-2024-21310</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21309</a>	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2024-21307</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2024-21306</a>	Microsoft Bluetooth Driver Spoofing Vulnerability
<a href="#">CVE-2024-21305</a>	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability
<a href="#">CVE-2024-20700</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2024-20699</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2024-20698</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20697</a>	Windows Libarchive Remote Code Execution Vulnerability
<a href="#">CVE-2024-20696</a>	Windows Libarchive Remote Code Execution Vulnerability
<a href="#">CVE-2024-20694</a>	Windows CoreMessaging Information Disclosure Vulnerability
<a href="#">CVE-2024-20692</a>	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
<a href="#">CVE-2024-20691</a>	Windows Themes Information Disclosure Vulnerability
<a href="#">CVE-2024-20690</a>	Windows Nearby Sharing Spoofing Vulnerability
<a href="#">CVE-2024-20687</a>	Microsoft AllJoyn API Denial of Service Vulnerability
<a href="#">CVE-2024-20683</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20682</a>	Windows Cryptographic Services Remote Code Execution Vulnerability
<a href="#">CVE-2024-20681</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20680</a>	No Vulnerability Name Found
<a href="#">CVE-2024-20674</a>	Windows Kerberos Security Feature Bypass Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2024-20666</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2024-20664</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2024-20663</a>	No Vulnerability Name Found
<a href="#">CVE-2024-20662</a>	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability
<a href="#">CVE-2024-20661</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2024-20660</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2024-20658</a>	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20657</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20655</a>	Microsoft Online Certificate Status Protocol (OCSP) Remote Code Execution Vulnerability
<a href="#">CVE-2024-20654</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2024-20653</a>	Microsoft Common Log File System Elevation of Privilege Vulnerability
<a href="#">CVE-2024-20652</a>	Windows HTML Platforms Security Feature Bypass Vulnerability
<a href="#">CVE-2024-0057</a>	NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability
<a href="#">CVE-2024-0056</a>	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability

## **December 2023:**

<a href="#">CVE-2023-36696</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36012</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36011</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36006</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-36005</a>	Windows Telephony Server Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36004</a>	Windows DPAPI (Data Protection Application Programming Interface) Spoofing Vulnerability
<a href="#">CVE-2023-36003</a>	XAML Diagnostics Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35644</a>	No Vulnerability Name Found
<a href="#">CVE-2023-35643</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-35642</a>	Internet Connection Sharing (ICS) Denial of Service Vulnerability
<a href="#">CVE-2023-35641</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35639</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-35638</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-35634</a>	Windows Bluetooth Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-35633</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35632</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35631</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35630</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35629</a>	0 Device Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-35628</a>	Windows MSHTML Platform Remote Code Execution Vulnerability
<a href="#">CVE-2023-35622</a>	Windows DNS Spoofing Vulnerability
<a href="#">CVE-2023-21740</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-20588</a>	AMD Speculative Leaks Security Notice

## **November 2023:**

<a href="#">CVE-2023-36719</a>	Microsoft Speech Application Programming Interface (SAPI) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36705</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36560</a>	NET Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36428</a>	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-36427</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36425</a>	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36424</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36423</a>	Microsoft Remote Registry Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-36408</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36407</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36406</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2023-36405</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36404</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36403</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36402</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-36401</a>	Microsoft Remote Registry Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-36400</a>	Windows HMAC Key Derivation Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36399</a>	Windows Storage Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36398</a>	Windows NTFS Information Disclosure Vulnerability
<a href="#">CVE-2023-36397</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36395</a>	Windows Deployment Services Denial of Service Vulnerability
<a href="#">CVE-2023-36394</a>	Windows Search Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36393</a>	Windows User Interface Application Core Remote Code Execution Vulnerability
<a href="#">CVE-2023-36392</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-36049</a>	No Vulnerability Name Found
<a href="#">CVE-2023-36047</a>	Windows Authentication Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36046</a>	Windows Authentication Denial of Service Vulnerability
<a href="#">CVE-2023-36036</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36033</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36028</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36025</a>	Windows SmartScreen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36017</a>	Windows Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2023-24023</a>	Mitre CVE-2023-24023 Bluetooth Vulnerability
<a href="#">CVE-2023-36008</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36014</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36022</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36024</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36026</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2023-36027</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36034</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-5480</a>	Chromium CVE-2023-5480 Inappropriate implementation in Payments
<a href="#">CVE-2023-5482</a>	Chromium CVE-2023-5482 Insufficient data validation in USB
<a href="#">CVE-2023-5849</a>	Chromium CVE-2023-5849 Integer overflow in USB
<a href="#">CVE-2023-5850</a>	Chromium CVE-2023-5850 Incorrect security UI in Downloads
<a href="#">CVE-2023-5851</a>	Chromium CVE-2023-5851 Inappropriate implementation in Downloads
<a href="#">CVE-2023-5852</a>	Chromium CVE-2023-5852 Use after free in Printing
<a href="#">CVE-2023-5853</a>	Chromium CVE-2023-5853 Incorrect security UI in Downloads
<a href="#">CVE-2023-5854</a>	Chromium CVE-2023-5854 Use after free in Profiles



<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-5855</a>	Chromium CVE-2023-5855 Use after free in Reading Mode
<a href="#">CVE-2023-5856</a>	Chromium CVE-2023-5856 Use after free in Side Panel
<a href="#">CVE-2023-5857</a>	Chromium CVE-2023-5857 Inappropriate implementation in Downloads
<a href="#">CVE-2023-5858</a>	Chromium CVE-2023-5858 Inappropriate implementation in WebApp Provider
<a href="#">CVE-2023-5859</a>	Chromium CVE-2023-5859 Incorrect security UI in Picture In Picture
<a href="#">CVE-2023-5996</a>	Chromium CVE-2023-5996 Use after free in WebAudio
<a href="#">CVE-2023-5997</a>	Chromium CVE-2023-5997 Use after free in Garbage Collection
<a href="#">CVE-2023-6112</a>	Chromium CVE-2023-6112 Use after free in Navigation
<a href="#">CVE-2023-44487</a>	HTTP/2 protocol allows a denial of service
<a href="#">CVE-2023-41774</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41773</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41772</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-41771</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41770</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41769</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41768</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41767</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-41766</a>	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-41765</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-38171</a>	Microsoft QUIC Denial of Service Vulnerability
<a href="#">CVE-2023-38166</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-38159</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36902</a>	Windows Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-36776</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36743</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36732</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36731</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36729</a>	Named Pipe File System Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36726</a>	Windows Internet Key Exchange (IKE) Extension Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36725</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36724</a>	Windows Power Management Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36723</a>	Windows Container Manager Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36722</a>	Active Directory Domain Services Information Disclosure Vulnerability
<a href="#">CVE-2023-36721</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36720</a>	Windows Mixed Reality Developer Tools Denial of Service Vulnerability
<a href="#">CVE-2023-36718</a>	Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability
<a href="#">CVE-2023-36717</a>	Windows Virtual Trusted Platform Module Denial of Service Vulnerability
<a href="#">CVE-2023-36713</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-36712</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36711</a>	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36710</a>	Windows Media Foundation Core Remote Code Execution Vulnerability
<a href="#">CVE-2023-36709</a>	Microsoft AllJoyn API Denial of Service Vulnerability
<a href="#">CVE-2023-36707</a>	Windows Deployment Services Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-36706</a>	Windows Deployment Services Information Disclosure Vulnerability
<a href="#">CVE-2023-36704</a>	Windows Setup Files Cleanup Remote Code Execution Vulnerability
<a href="#">CVE-2023-36703</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-36702</a>	Microsoft DirectMusic Remote Code Execution Vulnerability
<a href="#">CVE-2023-36701</a>	Microsoft Resilient File System (ReFS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36698</a>	Windows Kernel Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36697</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36606</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-36605</a>	Windows Named Pipe Filesystem Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36603</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-36602</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-36598</a>	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-36596</a>	Remote Procedure Call Information Disclosure Vulnerability
<a href="#">CVE-2023-36594</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36593</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36592</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36591</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36590</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36589</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36585</a>	Active Template Library Denial of Service Vulnerability
<a href="#">CVE-2023-36584</a>	Windows Mark of the Web Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36583</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36582</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36581</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-36579</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-36578</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36577</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-36576</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36575</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36574</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36573</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36572</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36571</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36570</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36567</a>	Windows Deployment Services Information Disclosure Vulnerability
<a href="#">CVE-2023-36564</a>	Windows Search Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36563</a>	Microsoft WordPad Information Disclosure Vulnerability
<a href="#">CVE-2023-36557</a>	PrintHTML API Remote Code Execution Vulnerability
<a href="#">CVE-2023-36438</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-36436</a>	Windows MSHTML Platform Remote Code Execution Vulnerability
<a href="#">CVE-2023-36435</a>	Microsoft QUIC Denial of Service Vulnerability
<a href="#">CVE-2023-36434</a>	Windows IIS Server Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36431</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-35349</a>	Microsoft Message Queuing Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-29348</a>	Windows Remote Desktop Gateway (RD Gateway) Information Disclosure Vulnerability
<a href="#">CVE-2023-38162</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-38162</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-38162</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-38162</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-38162</a>	DHCP Server Service Denial of Service Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38161</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38160</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38152</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-38150</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38149</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2023-38148</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-38148</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-38148</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-38148</a>	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-38147</a>	Windows Miracast Wireless Display Remote Code Execution Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-38139</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36805</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36804</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36803</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-36802</a>	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36802</a>	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36802</a>	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36802</a>	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36802</a>	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-36801</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-35355</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35355</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-35355</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35355</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35355</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-5346</a>	Type confusion in V8 in Google Chrome prior to 117.0.5938.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-4078</a>	Chromium: CVE-2023-4078 Inappropriate implementation in Extensions
<a href="#">CVE-2023-4077</a>	Chromium: CVE-2023-4077 Insufficient data validation in Extensions
<a href="#">CVE-2023-4076</a>	Chromium: CVE-2023-4076 Use after free in WebRTC
<a href="#">CVE-2023-4075</a>	Chromium: CVE-2023-4075 Use after free in Cast
<a href="#">CVE-2023-4074</a>	Chromium: CVE-2023-4074 Use after free in Blink Task Scheduling
<a href="#">CVE-2023-4073</a>	Chromium: CVE-2023-4073 Out of bounds memory access in ANGLE
<a href="#">CVE-2023-4072</a>	Chromium: CVE-2023-4072 Out of bounds read and write in WebGL
<a href="#">CVE-2023-4071</a>	Chromium: CVE-2023-4071 Heap buffer overflow in Visuals
<a href="#">CVE-2023-4070</a>	Chromium: CVE-2023-4070 Type Confusion in V8
<a href="#">CVE-2023-4069</a>	Chromium: CVE-2023-4069 Type Confusion in V8
<a href="#">CVE-2023-4068</a>	Chromium: CVE-2023-4068 Type Confusion in V8
<a href="#">CVE-2023-38254</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-38186</a>	Windows Mobile Device Management Elevation of Privilege Vulnerability Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-38184</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-38172</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-38157</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2023-38154</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36914</a>	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36913</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2023-36912</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-36911</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36910</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-36909</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-36908</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2023-36907</a>	Windows Cryptographic Services Information Disclosure Vulnerability
<a href="#">CVE-2023-36906</a>	Windows Cryptographic Services Information Disclosure Vulnerability Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability
<a href="#">CVE-2023-36905</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36904</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36903</a>	Windows System Assessment Tool Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36900</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36898</a>	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability
<a href="#">CVE-2023-36889</a>	Windows Group Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2023-36882</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-35387</a>	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35386</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35385</a>	Microsoft Message Queuing Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-35384</a>	Windows HTML Platforms Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35383</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2023-35382</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35381</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-35380</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35378</a>	Windows Projected File System Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35377</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-35376</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-35359</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35316</a>	Remote Procedure Call Runtime Information Disclosure Vulnerability
<a href="#">CVE-2023-20569</a>	This may result in speculative execution at an attacker-controlled address
<a href="#">CVE-2023-38187</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-3740</a>	Chromium: CVE-2023-3740 Insufficient validation of untrusted input in Themes
<a href="#">CVE-2023-3738</a>	Chromium: CVE-2023-3738 Inappropriate implementation in Autofill
<a href="#">CVE-2023-3737</a>	Chromium: CVE-2023-3737 Inappropriate implementation in Notifications
<a href="#">CVE-2023-3736</a>	Chromium: CVE-2023-3736 Inappropriate implementation in Custom Tabs
<a href="#">CVE-2023-3735</a>	Chromium: CVE-2023-3735 Inappropriate implementation in Web API Permission Prompts
<a href="#">CVE-2023-3734</a>	Chromium: CVE-2023-3734 Inappropriate implementation in Picture In Picture
<a href="#">CVE-2023-3733</a>	Chromium: CVE-2023-3733 Inappropriate implementation in WebApp Installs
<a href="#">CVE-2023-3732</a>	Chromium: CVE-2023-3732 Out of bounds memory access in Mojo
<a href="#">CVE-2023-3730</a>	Chromium: CVE-2023-3730 Use after free in Tab Groups
<a href="#">CVE-2023-3728</a>	Chromium: CVE-2023-3728 Use after free in WebRTC
<a href="#">CVE-2023-3727</a>	Chromium: CVE-2023-3727 Use after free in WebRTC
<a href="#">CVE-2023-36887</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-36884</a>	Office and Windows HTML Remote Code Execution Vulnerability
<a href="#">CVE-2023-36874</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-36871</a>	Azure Active Directory Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35392</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2023-35367</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35366</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35365</a>	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35364</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35363</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35362</a>	Windows Clip Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35361</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35360</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35358</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35357</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35356</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35353</a>	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35352</a>	Windows Remote Desktop Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35351</a>	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-35350</a>	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35348</a>	Active Directory Federation Service Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35347</a>	Microsoft Install Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35346</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-35345</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-35344</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-35343</a>	Windows Geolocation Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-35342</a>	Windows Image Acquisition Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35341</a>	Microsoft DirectMusic Information Disclosure Vulnerability
<a href="#">CVE-2023-35340</a>	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35339</a>	Windows CryptoAPI Denial of Service Vulnerability
<a href="#">CVE-2023-35338</a>	Windows Peer Name Resolution Protocol Denial of Service Vulnerability
<a href="#">CVE-2023-35337</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35336</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35332</a>	Windows Remote Desktop Protocol Security Feature Bypass
<a href="#">CVE-2023-35331</a>	Windows Local Security Authority (LSA) Denial of Service Vulnerability
<a href="#">CVE-2023-35330</a>	Windows Extended Negotiation Denial of Service Vulnerability
<a href="#">CVE-2023-35329</a>	Windows Authentication Denial of Service Vulnerability
<a href="#">CVE-2023-35328</a>	Windows Transaction Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35326</a>	Windows CDP User Components Information Disclosure Vulnerability
<a href="#">CVE-2023-35325</a>	Windows Print Spooler Information Disclosure Vulnerability
<a href="#">CVE-2023-35324</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-35323</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2023-35322</a>	Windows Deployment Services Remote Code Execution Vulnerability
<a href="#">CVE-2023-35321</a>	Windows Deployment Services Denial of Service Vulnerability
<a href="#">CVE-2023-35320</a>	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35319</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-35318</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-35317</a>	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35316</a>	Remote Procedure Call Runtime Information Disclosure Vulnerability
<a href="#">CVE-2023-35315</a>	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-35314</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-35313</a>	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability
<a href="#">CVE-2023-35312</a>	SYS Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35310</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-35309</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-35308</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-35306</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-35305</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35304</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35303</a>	USB Audio Class System Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-35302</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-35300</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-35299</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-35298</a>	sys Denial of Service Vulnerability
<a href="#">CVE-2023-35297</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-35296</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-33174</a>	Windows Cryptographic Information Disclosure Vulnerability
<a href="#">CVE-2023-33173</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33172</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33169</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33168</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33167</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33166</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33164</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-33163</a>	Windows Network Load Balancing Remote Code Execution Vulnerability
<a href="#">CVE-2023-33155</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-33154</a>	Windows Partition Management Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32085</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-32084</a>	sys Denial of Service Vulnerability
<a href="#">CVE-2023-32083</a>	Microsoft Failover Cluster Information Disclosure Vulnerability
<a href="#">CVE-2023-32057</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-32056</a>	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32055</a>	Active Template Library Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32054</a>	Volume Shadow Copy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32053</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32049</a>	Windows SmartScreen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-32046</a>	Windows MSHTML Platform Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32045</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-32044</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-32043</a>	Windows Remote Desktop Security Feature Bypass Vulnerability
<a href="#">CVE-2023-32042</a>	OLE Automation Information Disclosure Vulnerability
<a href="#">CVE-2023-32041</a>	Windows Update Orchestrator Service Information Disclosure Vulnerability
<a href="#">CVE-2023-32040</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-32039</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-32038</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-32037</a>	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-32035</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-32034</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-32033</a>	Microsoft Failover Cluster Remote Code Execution Vulnerability
<a href="#">CVE-2023-21756</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21526</a>	Windows Netlogon Information Disclosure Vulnerability
<a href="#">ADV230002</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">ADV230001</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-32030</a>	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-32022</a>	No Vulnerability Name Found
<a href="#">CVE-2023-32021</a>	Windows SMB Witness Service Security Feature Bypass Vulnerability
<a href="#">CVE-2023-32020</a>	Windows DNS Spoofing Vulnerability
<a href="#">CVE-2023-32019</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-32017</a>	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-32016</a>	Windows Installer Information Disclosure Vulnerability
<a href="#">CVE-2023-32015</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-32014</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-32013</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2023-32012</a>	Windows Container Manager Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32011</a>	Windows iSCSI Discovery Service Denial of Service Vulnerability
<a href="#">CVE-2023-32009</a>	Windows Collaborative Translation Framework Elevation of Privilege Vulnerability
<a href="#">CVE-2023-32008</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-29373</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-29372</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-29371</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29370</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-29369</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-29368</a>	Windows Filtering Platform Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29367</a>	iSCSI Target WMI Provider Remote Code Execution Vulnerability
<a href="#">CVE-2023-29366</a>	Windows Geolocation Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-29365</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-29364</a>	Windows Authentication Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29363</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-29362</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2023-29361</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29360</a>	Windows TPM Device Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29359</a>	GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29358</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29355</a>	DHCP Server Service Information Disclosure Vulnerability
<a href="#">CVE-2023-29352</a>	Windows Remote Desktop Security Feature Bypass Vulnerability
<a href="#">CVE-2023-29351</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29346</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29336</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29331</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-29326</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-29325</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2023-29324</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28283</a>	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28251</a>	Windows Driver Revocation List Security Feature Bypass Vulnerability
<a href="#">CVE-2023-24949</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24948</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24947</a>	Windows Bluetooth Driver Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-24946</a>	Windows Backup Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24945</a>	Windows iSCSI Target Service Information Disclosure Vulnerability
<a href="#">CVE-2023-24944</a>	Windows Bluetooth Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24943</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-24942</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-24941</a>	Windows Network File System Remote Code Execution Vulnerability
<a href="#">CVE-2023-24940</a>	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability
<a href="#">CVE-2023-24939</a>	Server for NFS Denial of Service Vulnerability
<a href="#">CVE-2023-24938</a>	Windows CryptoAPI Denial of Service Vulnerability
<a href="#">CVE-2023-24937</a>	Windows CryptoAPI Denial of Service Vulnerability
<a href="#">CVE-2023-24936</a>	Server for NFS Denial of Service Vulnerability
<a href="#">CVE-2023-24932</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2023-24905</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2023-24903</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-24902</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24901</a>	Windows NFS Portmapper Information Disclosure Vulnerability
<a href="#">CVE-2023-24900</a>	Windows NTLM Security Support Provider Information Disclosure Vulnerability
<a href="#">CVE-2023-24899</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24898</a>	Windows SMB Denial of Service Vulnerability
<a href="#">CVE-2023-24897</a>	Server for NFS Denial of Service Vulnerability
<a href="#">CVE-2023-24895</a>	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-33145</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2023-33143</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-3079</a>	Inappropriate implementation in Extensions API in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to spoof the contents of the UI via a crafted Chrome Extension. (Chromium security severity Low)
<a href="#">CVE-2023-2941</a>	Inappropriate implementation in Downloads in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2940</a>	Insufficient data validation in Installer in Google Chrome on Windows prior to 114.0.5735.90 allowed a local attacker to perform privilege escalation via crafted symbolic link. (Chromium security severity Medium)
<a href="#">CVE-2023-2939</a>	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2938</a>	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2937</a>	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2936</a>	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-2935</a>	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-29345</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2023-2934</a>	Out of bounds memory access in Mojo in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2933</a>	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity High)
<a href="#">CVE-2023-2932</a>	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity High)
<a href="#">CVE-2023-2931</a>	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity High)
<a href="#">CVE-2023-2930</a>	Use after free in Extensions in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2929</a>	Out of bounds write in Swiftshader in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2726</a>	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2725</a>	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2724</a>	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2723</a>	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2722</a>	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2721</a>	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Critical)
<a href="#">CVE-2023-33145</a>	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
<a href="#">CVE-2023-29336</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29325</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2023-29324</a>	Windows MSHTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28308</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28307</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28306</a>	Windows DNS Server Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-28305</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28302</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-28298</a>	Windows Kernel Denial of Service Vulnerability
<a href="#">CVE-2023-28297</a>	Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28293</a>	Windows Kernel Elevation of Privilege Vulnerability Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28283</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28278</a>	Windows DNS Server Information Disclosure Vulnerability
<a href="#">CVE-2023-28277</a>	Windows DNS Server Information Disclosure Vulnerability
<a href="#">CVE-2023-28276</a>	Windows Group Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28275</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28274</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28273</a>	Windows Clip Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28272</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28271</a>	Windows Kernel Memory Information Disclosure Vulnerability
<a href="#">CVE-2023-28270</a>	Windows Lock Screen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28269</a>	Windows Boot Manager Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28268</a>	Netlogon RPC Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28267</a>	Remote Desktop Protocol Client Information Disclosure Vulnerability
<a href="#">CVE-2023-28266</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-28256</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28255</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28254</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28253</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-28252</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28251</a>	Windows Driver Revocation List Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28250</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28249</a>	Windows Boot Manager Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28248</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28247</a>	Windows Network File System Information Disclosure Vulnerability
<a href="#">CVE-2023-28246</a>	Windows Registry Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28244</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28243</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-28241</a>	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
<a href="#">CVE-2023-28240</a>	Windows Network Load Balancing Remote Code Execution Vulnerability Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
<a href="#">CVE-2023-28238</a>	Windows Kernel Remote Code Execution Vulnerability
<a href="#">CVE-2023-28237</a>	Windows Kernel Remote Code Execution Vulnerability
<a href="#">CVE-2023-28236</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28235</a>	Windows Lock Screen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28234</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-28233</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-28232</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28231</a>	DHCP Server Service Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-28229</a>	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28228</a>	Windows Spoofing Vulnerability
<a href="#">CVE-2023-28227</a>	Windows Bluetooth Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-28226</a>	Windows Enroll Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28225</a>	Windows NTLM Elevation of Privilege Vulnerability Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28224</a>	Windows Domain Name Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-28223</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28222</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28221</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28220</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28219</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28218</a>	Windows Network Address Translation (NAT) Denial of Service Vulnerability
<a href="#">CVE-2023-28217</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28216</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24949</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24948</a>	Windows Bluetooth Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24947</a>	Windows Backup Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24946</a>	Windows iSCSI Target Service Information Disclosure Vulnerability
<a href="#">CVE-2023-24945</a>	Windows Bluetooth Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24944</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-24943</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-24942</a>	Windows Network File System Remote Code Execution Vulnerability
<a href="#">CVE-2023-24941</a>	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability
<a href="#">CVE-2023-24940</a>	Server for NFS Denial of Service Vulnerability
<a href="#">CVE-2023-24939</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2023-24932</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-24931</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24929</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24928</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24927</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24926</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24925</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24924</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24912</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24905</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2023-24903</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-24902</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24901</a>	Windows NFS Portmapper Information Disclosure Vulnerability
<a href="#">CVE-2023-24900</a>	Windows NTLM Security Support Provider Information Disclosure Vulnerability
<a href="#">CVE-2023-24899</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24898</a>	Windows SMB Denial of Service Vulnerability
<a href="#">CVE-2023-24887</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24886</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-24885</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24884</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24883</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-21769</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-21729</a>	Remote Procedure Call Runtime Information Disclosure Vulnerability
<a href="#">CVE-2023-21727</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-21554</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-29354</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2023-29350</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-29334</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2023-24935</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-2468</a>	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-2467</a>	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-2466</a>	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2465</a>	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2464</a>	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2463</a>	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2462</a>	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2460</a>	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2459</a>	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-2137</a>	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2136</a>	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-2135</a>	

<http://buildings.honeywell.com/security>

- [CVE-2023-2134](#) Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
- [CVE-2023-2133](#) Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
- [CVE-2023-2033](#) Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
- [CVE-2023-1823](#) Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1822](#) Incorrect security UI in Navigation in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1821](#) Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1820](#) Heap buffer overflow in Browser History in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1819](#) Out of bounds read in Accessibility in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1818](#) Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1817](#) Insufficient policy enforcement in Intents in Google Chrome on Android prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1816](#) Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1815](#) Use after free in Networking APIs in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1814](#) Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1813](#) Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1812](#) Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1811](#) Use after free in Frames in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)



<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-1810</a>	Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-28308</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28307</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28306</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28305</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28302</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-28298</a>	Windows Kernel Denial of Service Vulnerability
<a href="#">CVE-2023-28297</a>	Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28293</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28278</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28277</a>	Windows DNS Server Information Disclosure Vulnerability
<a href="#">CVE-2023-28276</a>	Windows Group Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28275</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28274</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28273</a>	Windows Clip Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28272</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28271</a>	Windows Kernel Memory Information Disclosure Vulnerability
<a href="#">CVE-2023-28270</a>	Windows Lock Screen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28269</a>	Windows Boot Manager Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28268</a>	Netlogon RPC Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28267</a>	Remote Desktop Protocol Client Information Disclosure Vulnerability
<a href="#">CVE-2023-28266</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-28256</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28255</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28254</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-28253</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-28252</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28250</a>	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28249</a>	Windows Boot Manager Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28248</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28247</a>	Windows Network File System Information Disclosure Vulnerability
<a href="#">CVE-2023-28246</a>	Windows Registry Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28244</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28243</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-28241</a>	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
<a href="#">CVE-2023-28240</a>	Windows Network Load Balancing Remote Code Execution Vulnerability
<a href="#">CVE-2023-28238</a>	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
<a href="#">CVE-2023-28237</a>	Windows Kernel Remote Code Execution Vulnerability
<a href="#">CVE-2023-28236</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28235</a>	Windows Lock Screen Security Feature Bypass Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-28234</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-28233</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-28232</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28231</a>	DHCP Server Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-28229</a>	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28228</a>	Windows Spoofing Vulnerability
<a href="#">CVE-2023-28227</a>	Windows Bluetooth Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-28226</a>	Windows Enroll Engine Security Feature Bypass Vulnerability
<a href="#">CVE-2023-28225</a>	Windows NTLM Elevation of Privilege Vulnerability Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
<a href="#">CVE-2023-28224</a>	Windows Domain Name Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-28223</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28222</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28221</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28220</a>	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-28219</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28218</a>	Windows Network Address Translation (NAT) Denial of Service Vulnerability
<a href="#">CVE-2023-28217</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-28216</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-24931</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24929</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24928</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24927</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24926</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24925</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24924</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24914</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24912</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24887</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24886</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24885</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24884</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24883</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-21769</a>	Microsoft Message Queuing Denial of Service Vulnerability
<a href="#">CVE-2023-21729</a>	Remote Procedure Call Runtime Information Disclosure Vulnerability
<a href="#">CVE-2023-21727</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-21554</a>	Microsoft Message Queuing Remote Code Execution Vulnerability
<a href="#">CVE-2023-24935</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-1823</a>	Incorrect security UI in Navigation in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-1822</a>	

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-1821</a>	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity Low)
<a href="#">CVE-2023-1820</a>	Heap buffer overflow in Browser History in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1819</a>	Out of bounds read in Accessibility in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1818</a>	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1817</a>	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1816</a>	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1815</a>	Use after free in Networking APIs in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1814</a>	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1813</a>	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1812</a>	Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity Medium)
<a href="#">CVE-2023-1811</a>	Use after free in Frames in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1810</a>	Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-24913</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24911</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24910</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24909</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24908</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-24907</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24906</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24892</a>	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability
<a href="#">CVE-2023-24880</a>	Windows SmartScreen Security Feature Bypass Vulnerability
<a href="#">CVE-2023-24876</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24872</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-24871</a>	Windows Bluetooth Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-24870</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24869</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-24868</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24867</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-24866</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24865</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24864</a>	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24863</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24862</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-24861</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-24859</a>	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
<a href="#">CVE-2023-24858</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24857</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-24856</a>	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
<a href="#">CVE-2023-23423</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23422</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23421</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23420</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23417</a>	Windows Partition Management Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23416</a>	Windows Cryptographic Services Remote Code Execution Vulnerability
<a href="#">CVE-2023-23415</a>	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
<a href="#">CVE-2023-23414</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-23413</a>	Windows Accounts Picture Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23411</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2023-23410</a>	sys Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23409</a>	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
<a href="#">CVE-2023-23407</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-23406</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2023-23405</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2023-23404</a>	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-23403</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-23402</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-23401</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-23394</a>	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability
<a href="#">CVE-2023-23393</a>	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23392</a>	HTTP Protocol Stack Remote Code Execution Vulnerability
<a href="#">CVE-2023-23388</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-23385</a>	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21708</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

- [CVE-2023-1236](#) Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to spoof the origin of an iframe via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1235](#) Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted UI interaction. (Chromium security severity Low)
- [CVE-2023-1234](#) Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1233](#) Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from API via a crafted Chrome Extension. (Chromium security severity Low)
- [CVE-2023-1232](#) Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to obtain potentially sensitive information from API via a crafted HTML page. (Chromium security severity Low)
- [CVE-2023-1231](#) Inappropriate implementation in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1230](#) Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1229](#) Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1228](#) Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1224](#) Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1223](#) Insufficient policy enforcement in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1222](#) Heap buffer overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity Medium)
- [CVE-2023-1221](#) Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity Medium)
- [CVE-2023-1220](#) Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
- [CVE-2023-1219](#) Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-1218</a>	Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1217</a>	Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1216</a>	Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convinced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1215</a>	Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1214</a>	Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1213</a>	Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
<a href="#">CVE-2023-1018</a>	0's Module Library allowing a 2-byte read past the end of a TPM2
<a href="#">CVE-2023-1017</a>	0's Module Library allowing writing of a 2-byte data past the end of TPM2
<a href="#">CVE-2023-21808</a>	NET and Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2023-21802</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2023-21803</a>	Windows iSCSI Discovery Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-21804</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21805</a>	Windows MSHTML Platform Remote Code Execution Vulnerability
<a href="#">CVE-2023-21688</a>	NT OS Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21820</a>	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21700</a>	Windows iSCSI Discovery Service Denial of Service Vulnerability
<a href="#">CVE-2023-21689</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21722</a>	NET Framework Denial of Service Vulnerability
<a href="#">CVE-2023-21701</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability
<a href="#">CVE-2023-21822</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21823</a>	Windows Graphics Component Remote Code Execution Vulnerability
<a href="#">CVE-2023-21702</a>	Windows iSCSI Service Denial of Service Vulnerability
<a href="#">CVE-2023-21801</a>	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-21684</a>	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-21685</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-21686</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-21691</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability
<a href="#">CVE-2023-21692</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21693</a>	Microsoft PostScript Printer Driver Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-23376</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21694</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2023-21690</a>	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21817</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21818</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-21819</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-21813</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2023-21816</a>	Windows Active Directory Domain Services API Denial of Service Vulnerability
<a href="#">CVE-2023-21699</a>	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
<a href="#">CVE-2023-21798</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-21799</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-21811</a>	Windows iSCSI Service Denial of Service Vulnerability
<a href="#">CVE-2023-21812</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21695</a>	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
<a href="#">CVE-2023-21697</a>	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
<a href="#">CVE-2023-21797</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-0700</a>	Chromium:CVE-2023-0700 Inappropriate implementation in Download
<a href="#">CVE-2023-0701</a>	Chromium:CVE-2023-0701 Heap buffer overflow in WebUI
<a href="#">CVE-2023-0698</a>	Chromium:CVE-2023-0698 Out of bounds read in WebRTC
<a href="#">CVE-2023-0699</a>	Chromium:CVE-2023-0699 Use after free in GPU
<a href="#">CVE-2023-0704</a>	Chromium:CVE-2023-0704 Insufficient policy enforcement in DevTools
<a href="#">CVE-2023-0705</a>	Chromium:CVE-2023-0705 Integer overflow in Core
<a href="#">CVE-2023-0702</a>	Chromium:CVE-2023-0702 Type Confusion in Data Transfer
<a href="#">CVE-2023-0703</a>	Chromium:CVE-2023-0703 Type Confusion in DevTools
<a href="#">CVE-2023-0696</a>	Chromium:CVE-2023-0696 Type Confusion in V8
<a href="#">CVE-2023-21794</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2023-0697</a>	Chromium: CVE-2023-0697 Inappropriate implementation in Full screen mode
<a href="#">CVE-2023-21720</a>	Microsoft Edge (Chromium-based) Tampering Vulnerability
<a href="#">CVE-2023-21687</a>	HTTP.sys Information Disclosure Vulnerability
<a href="#">CVE-2023-21796</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21795</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21776</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2023-21775</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21775</a>	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21774</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21773</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21772</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21771</a>	Windows Local Session Manager (LSM) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21768</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21767</a>	Windows Overlay Filter Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21766</a>	Windows Overlay Filter Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-21765</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21760</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21759</a>	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability
<a href="#">CVE-2023-21758</a>	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
<a href="#">CVE-2023-21757</a>	Windows Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability
<a href="#">CVE-2023-21755</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21754</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21753</a>	Event Tracing for Windows Information Disclosure Vulnerability
<a href="#">CVE-2023-21752</a>	Windows Backup Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21750</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21749</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21748</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21747</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21746</a>	Windows NTLM Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21739</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21733</a>	Windows Bind Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21732</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2023-21730</a>	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21728</a>	Windows Netlogon Denial of Service Vulnerability
<a href="#">CVE-2023-21726</a>	Windows Credential Manager User Interface Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21724</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21719</a>	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
<a href="#">CVE-2023-21683</a>	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
<a href="#">CVE-2023-21682</a>	Windows Point-to-Point Protocol (PPP) Information Disclosure Vulnerability
<a href="#">CVE-2023-21681</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2023-21680</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21679</a>	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21678</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21677</a>	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
<a href="#">CVE-2023-21676</a>	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21675</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21674</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21563</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2023-21561</a>	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21560</a>	Windows Boot Manager Security Feature Bypass Vulnerability
<a href="#">CVE-2023-21559</a>	Windows Cryptographic Information Disclosure Vulnerability
<a href="#">CVE-2023-21558</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21557</a>	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
<a href="#">CVE-2023-21556</a>	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21555</a>	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21552</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21551</a>	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21550</a>	Windows Cryptographic Information Disclosure Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2023-21549</a>	Windows SMB Witness Service Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21548</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21547</a>	Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability
<a href="#">CVE-2023-21546</a>	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21543</a>	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21542</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21541</a>	Windows Task Scheduler Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21540</a>	Windows Cryptographic Information Disclosure Vulnerability
<a href="#">CVE-2023-21539</a>	Windows Authentication Remote Code Execution Vulnerability
<a href="#">CVE-2023-21537</a>	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21536</a>	Event Tracing for Windows Information Disclosure Vulnerability
<a href="#">CVE-2023-21535</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2023-21532</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2023-21527</a>	Windows iSCSI Service Denial of Service Vulnerability
<a href="#">CVE-2023-21525</a>	Remote Procedure Call Runtime Denial of Service Vulnerability
<a href="#">CVE-2023-21524</a>	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
<a href="#">CVE-2023-0141</a>	Chromium:CVE-2023-0141: Insufficient policy enforcement in CORS
<a href="#">CVE-2023-0140</a>	Chromium:CVE-2023-0140: Inappropriate implementation in File System API
<a href="#">CVE-2023-0139</a>	Chromium:CVE-2023-0139: Insufficient validation of untrusted input in Downloads
<a href="#">CVE-2023-0138</a>	Chromium:CVE-2023-0138: Heap buffer overflow in libphonenumber
<a href="#">CVE-2023-0136</a>	Chromium:CVE-2023-0136: Inappropriate implementation in Fullscreen API
<a href="#">CVE-2023-0135</a>	Chromium:CVE-2023-0135: Use after free in Cart
<a href="#">CVE-2023-0134</a>	Chromium:CVE-2023-0134: Use after free in Cart
<a href="#">CVE-2023-0133</a>	Chromium:CVE-2023-0133: Inappropriate implementation in Permission prompts
<a href="#">CVE-2023-0132</a>	Chromium:CVE-2023-0132: Inappropriate implementation in Permission prompts
<a href="#">CVE-2023-0131</a>	Chromium:CVE-2023-0131: Inappropriate implementation in iframe Sandbox
<a href="#">CVE-2023-0130</a>	Chromium:CVE-2023-0130: Inappropriate implementation in Fullscreen API
<a href="#">CVE-2023-0129</a>	Chromium:CVE-2023-0129: Heap buffer overflow in Network Service
<a href="#">CVE-2022-41113</a>	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
<a href="#">ADV220005</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability

## **2022 – Microsoft® Patches Tested with Pro-Watch:**

<a href="#">CVE-2022-44708</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44707</a>	Windows Kernel Denial of Service Vulnerability
<a href="#">CVE-2022-44698</a>	Windows SmartScreen Security Feature Bypass Vulnerability
<a href="#">CVE-2022-44697</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44689</a>	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44688</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2022-44683</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44682</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2022-44681</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44680</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44679</a>	Windows Graphics Component Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-44678</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44677</a>	Windows Projected File System Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44676</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-44675</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44674</a>	Windows Bluetooth Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-44673</a>	Windows Client Server Run-Time Subsystem (CSRSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44671</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44670</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-44669</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2022-44668</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2022-44667</a>	Windows Media Remote Code Execution Vulnerability
<a href="#">CVE-2022-44666</a>	Windows Contacts Remote Code Execution Vulnerability
<a href="#">CVE-2022-4440</a>	Chromium: CVE-2022-4440 Use after free in Profiles
<a href="#">CVE-2022-4439</a>	Chromium: CVE-2022-4439 Use after free in Aura
<a href="#">CVE-2022-4438</a>	Chromium: CVE-2022-4438 Use after free in Blink Frames
<a href="#">CVE-2022-4437</a>	Chromium: CVE-2022-4437 Use after free in Mojo IPC
<a href="#">CVE-2022-4436</a>	Chromium: CVE-2022-4436 Use after free in Blink Media
<a href="#">CVE-2022-4195</a>	Chromium: CVE-2022-4195 Insufficient policy enforcement in Safe Browsing
<a href="#">CVE-2022-4194</a>	Chromium: CVE-2022-4194 Use after free in Accessibility
<a href="#">CVE-2022-4193</a>	Chromium: CVE-2022-4193 Insufficient policy enforcement in File System API
<a href="#">CVE-2022-4192</a>	Chromium: CVE-2022-4192 Use after free in Live Caption
<a href="#">CVE-2022-4191</a>	Chromium: CVE-2022-4191 Use after free in Sign-In
<a href="#">CVE-2022-4190</a>	Chromium: CVE-2022-4190 Insufficient data validation in Directory
<a href="#">CVE-2022-4189</a>	Chromium: CVE-2022-4189 Insufficient policy enforcement in DevTools
<a href="#">CVE-2022-4188</a>	Chromium: CVE-2022-4188 Insufficient validation of untrusted input in CORS
<a href="#">CVE-2022-4187</a>	Chromium: CVE-2022-4187 Insufficient policy enforcement in DevTools
<a href="#">CVE-2022-4186</a>	Chromium: CVE-2022-4186 Insufficient validation of untrusted input in Downloads
<a href="#">CVE-2022-4185</a>	Chromium: CVE-2022-4185 Inappropriate implementation in Navigation
<a href="#">CVE-2022-4184</a>	Chromium: CVE-2022-4184 Insufficient policy enforcement in Autofill
<a href="#">CVE-2022-4183</a>	Chromium: CVE-2022-4183 Insufficient policy enforcement in Popup Blocker
<a href="#">CVE-2022-4182</a>	Chromium: CVE-2022-4182 Inappropriate implementation in Fenced Frames
<a href="#">CVE-2022-4181</a>	Chromium: CVE-2022-4181 Use after free in Forms
<a href="#">CVE-2022-4180</a>	Chromium: CVE-2022-4180 Use after free in Mojo
<a href="#">CVE-2022-4179</a>	Chromium: CVE-2022-4179 Use after free in Audio
<a href="#">CVE-2022-4178</a>	Chromium: CVE-2022-4178 Use after free in Mojo
<a href="#">CVE-2022-4177</a>	Chromium: CVE-2022-4177 Use after free in Extensions
<a href="#">CVE-2022-4175</a>	Chromium: CVE-2022-4175 Use after free in Camera Capture
<a href="#">CVE-2022-4174</a>	Chromium: CVE-2022-4174 Type Confusion in V8
<a href="#">CVE-2022-41121</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41115</a>	Microsoft Edge (Chromium-based) Update Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41094</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41089</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2022-41077</a>	Windows Fax Compose Form Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41076</a>	PowerShell Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-41074</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2022-37967</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">ADV220005</a>	Guidance on Microsoft Signed Drivers Being Used Maliciously
<a href="#">CVE-2022-41128</a>	Windows Scripting Languages Remote Code Execution Vulnerability
<a href="#">CVE-2022-41125</a>	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41118</a>	Windows Scripting Languages Remote Code Execution Vulnerability
<a href="#">CVE-2022-41114</a>	Windows Bind Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41113</a>	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41109</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41102</a>	Windows Overlay Filter Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41101</a>	Windows Overlay Filter Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41100</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41099</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2022-41098</a>	Windows GDI+ Information Disclosure Vulnerability
<a href="#">CVE-2022-41097</a>	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability
<a href="#">CVE-2022-41096</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41095</a>	Windows Digital Media Receiver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41093</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41092</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41091</a>	Windows Mark of the Web Security Feature Bypass Vulnerability
<a href="#">CVE-2022-41090</a>	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
<a href="#">CVE-2022-41088</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-41086</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41073</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41064</a>	.NET Framework Information Disclosure Vulnerability
<a href="#">CVE-2022-41058</a>	Windows Network Address Translation (NAT) Denial of Service Vulnerability
<a href="#">CVE-2022-41057</a>	Windows HTTP.sys Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41056</a>	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability
<a href="#">CVE-2022-41055</a>	Windows Human Interface Device Information Disclosure Vulnerability
<a href="#">CVE-2022-41054</a>	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41053</a>	Windows Kerberos Denial of Service Vulnerability
<a href="#">CVE-2022-41052</a>	Windows Graphics Component Remote Code Execution Vulnerability
<a href="#">CVE-2022-41050</a>	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41049</a>	Windows Mark of the Web Security Feature Bypass Vulnerability
<a href="#">CVE-2022-41048</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2022-41047</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2022-41045</a>	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41039</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-3890</a>	Chromium: CVE-2022-3890 Heap buffer overflow in Crashpad
<a href="#">CVE-2022-3889</a>	Chromium: CVE-2022-3889 Type Confusion in V8
<a href="#">CVE-2022-3888</a>	CVE-2022-3888 Use after free in WebCodecs
<a href="#">CVE-2022-3887</a>	CVE-2022-3887 Use after free in Web Workers
<a href="#">CVE-2022-3886</a>	CVE-2022-3886 Use after free in Speech Recognition

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-3885</a>	CVE-2022-3885 Use after free in V8
<a href="#">CVE-2022-38023</a>	Netlogon RPC Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38015</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2022-37992</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37967</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37966</a>	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23824</a>	AMD: CVE-2022-23824 IBPB and Return Address Predictor Interactions
<a href="#">CVE-2022-41081</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-41033</a>	Windows COM+ Event System Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38051</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38050</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38047</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-38046</a>	Web Account Manager Information Disclosure Vulnerability
<a href="#">CVE-2022-38045</a>	Windows Server Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38044</a>	Windows CD-ROM File System Driver Remote Code Execution Vulnerability
<a href="#">CVE-2022-38043</a>	Windows Security Support Provider Interface Information Disclosure Vulnerability
<a href="#">CVE-2022-38042</a>	Active Directory Domain Services Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38041</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2022-38040</a>	Microsoft ODBC Driver Remote Code Execution Vulnerability
<a href="#">CVE-2022-38039</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38038</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38037</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38034</a>	Windows Workstation Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38033</a>	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability
<a href="#">CVE-2022-38032</a>	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability
<a href="#">CVE-2022-38031</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-38030</a>	Windows USB Serial Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-38029</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38028</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38027</a>	Windows Storage Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38026</a>	Windows DHCP Client Information Disclosure Vulnerability
<a href="#">CVE-2022-38022</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38021</a>	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38016</a>	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38003</a>	Windows Resilient File System Elevation of Privilege
<a href="#">CVE-2022-38000</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-37999</a>	Windows Group Policy Preference Client Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37998</a>	Windows Local Session Manager (LSM) Denial of Service Vulnerability
<a href="#">CVE-2022-37997</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37996</a>	Windows Kernel Memory Information Disclosure Vulnerability
<a href="#">CVE-2022-37995</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37994</a>	Windows Group Policy Preference Client Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37993</a>	Windows Group Policy Preference Client Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-37991</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37990</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37989</a>	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37988</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37987</a>	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37986</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37985</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2022-37984</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37984</a>	Windows WLAN Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37983</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37982</a>	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-37981</a>	Windows Event Logging Service Denial of Service Vulnerability
<a href="#">CVE-2022-37980</a>	Windows DHCP Client Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37979</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37978</a>	Windows Active Directory Certificate Services Security Feature Bypass
<a href="#">CVE-2022-37977</a>	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability
<a href="#">CVE-2022-37976</a>	Active Directory Certificate Services Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37975</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37974</a>	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability
<a href="#">CVE-2022-37973</a>	Windows Local Session Manager (LSM) Denial of Service Vulnerability
<a href="#">CVE-2022-37970</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37965</a>	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
<a href="#">CVE-2022-35770</a>	Windows NTLM Spoofing Vulnerability
<a href="#">CVE-2022-33645</a>	Windows TCP/IP Driver Denial of Service Vulnerability
<a href="#">CVE-2022-33635</a>	Windows GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2022-33634</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-30198</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-24504</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-22035</a>	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
<a href="#">CVE-2022-41082</a>	Microsoft Exchange Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-41040</a>	Microsoft Exchange Server Elevation of Privilege Vulnerability
<a href="#">CVE-2022-41035</a>	Microsoft Edge (Chromium-based) Spoofing Vulnerability
<a href="#">CVE-2022-38006</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2022-38005</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-38004</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2022-37972</a>	Microsoft Endpoint Configuration Manager Spoofing Vulnerability
<a href="#">CVE-2022-37959</a>	Network Device Enrollment Service (NDES) Security Feature Bypass Vulnerability SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Information Disclosure Vulnerability
<a href="#">CVE-2022-37958</a>	
<a href="#">CVE-2022-37957</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37956</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-37955</a>	Windows Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35803</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-3373</a>	Chromium: CVE-2022-3373 Out of bounds write in V8
<a href="#">CVE-2022-3370</a>	Chromium: CVE-2022-3370 Use after free in Custom Elements
<a href="#">CVE-2022-3317</a>	Chromium: CVE-2022-3317 Insufficient validation of untrusted input in Intents
<a href="#">CVE-2022-3316</a>	Chromium: CVE-2022-3316 Insufficient validation of untrusted input in Safe Browsing
<a href="#">CVE-2022-3315</a>	Chromium: CVE-2022-3315 Type confusion in Blink
<a href="#">CVE-2022-3313</a>	Chromium: CVE-2022-3313 Incorrect security UI in Full Screen
<a href="#">CVE-2022-3311</a>	Chromium: CVE-2022-3311 Use after free in Import
<a href="#">CVE-2022-3310</a>	Chromium: CVE-2022-3310 Insufficient policy enforcement in Custom Tabs
<a href="#">CVE-2022-3308</a>	Chromium: CVE-2022-3308 Insufficient policy enforcement in Developer Tools
<a href="#">CVE-2022-3307</a>	Chromium: CVE-2022-3307 Use after free in Media
<a href="#">CVE-2022-3304</a>	Chromium: CVE-2022-3304 Use after free in CSS
<a href="#">CVE-2022-3200</a>	Chromium: CVE-2022-3200 Heap buffer overflow in Internals
<a href="#">CVE-2022-3199</a>	Chromium: CVE-2022-3199 Use after free in Frames
<a href="#">CVE-2022-3198</a>	Chromium: CVE-2022-3198 Use after free in PDF
<a href="#">CVE-2022-3197</a>	Chromium: CVE-2022-3197 Use after free in PDF
<a href="#">CVE-2022-3196</a>	Chromium: CVE-2022-3196 Use after free in PDF
<a href="#">CVE-2022-3195</a>	Chromium: CVE-2022-3195 Out of bounds write in Storage
<a href="#">CVE-2022-26929</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2022-35820</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35798</a>	Azure Arc Jumpstart Information Disclosure Vulnerability
<a href="#">CVE-2022-35797</a>	Windows Hello Security Feature Bypass Vulnerability
<a href="#">CVE-2022-35795</a>	Windows Error Reporting Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35794</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-35793</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35792</a>	Storage Spaces Direct Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35771</a>	Windows Defender Credential Guard Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35769</a>	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability
<a href="#">CVE-2022-35768</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35767</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-35766</a>	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-35765</a>	Storage Spaces Direct Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35764</a>	Storage Spaces Direct Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35763</a>	Storage Spaces Direct Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35760</a>	Microsoft ATA Port Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-35754</a>	Unified Write Filter Elevation of Privilege Vulnerability
<a href="#">CVE-2022-34703</a>	Windows Partition Management Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-34303</a>	CERT/CC: CVE-20220-34303 Crypto Pro Boot Loader Bypass
<a href="#">CVE-2022-33680</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33672</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33671</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33670</a>	Windows Partition Management Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33669</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33668</a>	Azure Site Recovery Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-33667</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33666</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33665</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33664</a>	Azure Site Recovery Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33639</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-33638</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-32230</a>	Windows SMB Denial of Service Vulnerability
<a href="#">CVE-2022-30193</a>	AV1 Video Extension Remote Code Execution Vulnerability
<a href="#">CVE-2022-30192</a>	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30188</a>	HEVC Video Extensions Remote Code Execution Vulnerability
<a href="#">CVE-2022-30184</a>	.NET and Visual Studio Information Disclosure Vulnerability
<a href="#">CVE-2022-30180</a>	Azure RTOS GUIX Studio Information Disclosure Vulnerability
<a href="#">CVE-2022-30179</a>	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
<a href="#">CVE-2022-30177</a>	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
<a href="#">CVE-2022-30166</a>	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30165</a>	Windows Kerberos Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30164</a>	Kerberos AppContainer Security Feature Bypass Vulnerability
<a href="#">CVE-2022-30163</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2022-30162</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2022-30161</a>	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-30160</a>	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30155</a>	Windows Kernel Denial of Service Vulnerability
<a href="#">CVE-2022-30154</a>	Microsoft File Server Shadow Copy Agent Service (RVSS) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30153</a>	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
<a href="#">CVE-2022-30138</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-30130</a>	.NET Framework Denial of Service Vulnerability
<a href="#">CVE-2022-29149</a>	Azure Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-29143</a>	Microsoft SQL Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-29142</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-29141</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29140</a>	Windows Print Spooler Information Disclosure Vulnerability
<a href="#">CVE-2022-29139</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29138</a>	Windows Clustered Shared Volume Elevation of Privilege Vulnerability
<a href="#">CVE-2022-29137</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29135</a>	Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
<a href="#">CVE-2022-29134</a>	Windows Clustered Shared Volume Information Disclosure Vulnerability
<a href="#">CVE-2022-29132</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-29131</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29130</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29129</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-29128</a>	Windows LDAP Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-27776</a>	HackerOne: CVE-2022-27776 Insufficiently protected credentials vulnerability might leak authentication or cookie header data
<a href="#">CVE-2022-26920</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2022-26919</a>	Windows LDAP Remote Code Execution Vulnerability
<a href="#">CVE-2022-26918</a>	Windows Fax Compose Form Remote Code Execution Vulnerability
<a href="#">CVE-2022-26917</a>	Windows Fax Compose Form Remote Code Execution Vulnerability
<a href="#">CVE-2022-26916</a>	Windows Fax Compose Form Remote Code Execution Vulnerability
<a href="#">CVE-2022-26915</a>	Windows Secure Channel Denial of Service Vulnerability
<a href="#">CVE-2022-26904</a>	Windows User Profile Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26832</a>	.NET Framework Denial of Service Vulnerability
<a href="#">CVE-2022-26831</a>	Windows LDAP Denial of Service Vulnerability
<a href="#">CVE-2022-26828</a>	Windows Bluetooth Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26827</a>	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26825</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26824</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26823</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26822</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26821</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26812</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26811</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-26810</a>	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26809</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2022-26808</a>	Windows File Explorer Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26807</a>	Windows Work Folder Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26803</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26802</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26801</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26798</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26797</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26796</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26794</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26792</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26790</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26789</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26787</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-26786</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-24525</a>	Windows Update Stack Elevation of Privilege Vulnerability
<a href="#">CVE-2022-24512</a>	.NET and Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2022-24507</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2022-24503</a>	Remote Desktop Protocol Client Information Disclosure Vulnerability
<a href="#">CVE-2022-24502</a>	Windows HTML Platforms Security Feature Bypass Vulnerability
<a href="#">CVE-2022-24464</a>	.NET and Visual Studio Denial of Service Vulnerability
<a href="#">CVE-2022-24460</a>	Tablet Windows User Interface Application Elevation of Privilege Vulnerability
<a href="#">CVE-2022-24459</a>	Windows Fax and Scan Service Elevation of Privilege Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-24455</a>	Windows CD-ROM Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-24454</a>	Windows Security Support Provider Interface Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23825</a>	AMD: CVE-2022-23825 AMD CPU Branch Type Confusion
<a href="#">CVE-2022-23299</a>	Windows PDEV Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23298</a>	Windows NT OS Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23297</a>	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-23296</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23294</a>	Windows Event Tracing Remote Code Execution Vulnerability
<a href="#">CVE-2022-23293</a>	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23291</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23290</a>	Windows Inking COM Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23288</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23287</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23285</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2022-23284</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23283</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2022-23281</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-23278</a>	Microsoft Defender for Endpoint Spoofing Vulnerability
<a href="#">CVE-2022-23253</a>	Point-to-Point Tunneling Protocol Denial of Service Vulnerability
<a href="#">CVE-2022-22050</a>	Windows Fax Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22049</a>	Windows CSRSS Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22048</a>	BitLocker Security Feature Bypass Vulnerability
<a href="#">CVE-2022-22047</a>	Windows CSRSS Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22045</a>	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22043</a>	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22042</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2022-22041</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22040</a>	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability
<a href="#">CVE-2022-22039</a>	Windows Network File System Remote Code Execution Vulnerability
<a href="#">CVE-2022-22019</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2022-22010</a>	Media Foundation Information Disclosure Vulnerability
<a href="#">CVE-2022-22002</a>	Windows User Account Profile Picture Denial of Service Vulnerability
<a href="#">CVE-2022-22001</a>	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2022-22000</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21999</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21998</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-21997</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21995</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2022-21994</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21993</a>	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
<a href="#">CVE-2022-21992</a>	Windows Mobile Device Management Remote Code Execution Vulnerability
<a href="#">CVE-2022-21989</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21981</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21977</a>	Media Foundation Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-21963</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21962</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21961</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21960</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21959</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21958</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21928</a>	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
<a href="#">CVE-2022-21924</a>	Workstation Service Remote Protocol Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21913</a>	Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass
<a href="#">CVE-2022-21911</a>	.NET Framework Denial of Service Vulnerability
<a href="#">CVE-2022-21908</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21907</a>	HTTP Protocol Stack Remote Code Execution Vulnerability
<a href="#">CVE-2022-21906</a>	Windows Defender Application Control Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21905</a>	Windows Hyper-V Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21904</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2022-21903</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21902</a>	Windows DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21901</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21900</a>	Windows Hyper-V Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21899</a>	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21898</a>	DirectX Graphics Kernel Remote Code Execution Vulnerability
<a href="#">CVE-2022-21897</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21894</a>	Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2022-21890</a>	Windows IKE Extension Denial of Service Vulnerability
<a href="#">CVE-2022-21889</a>	Windows IKE Extension Denial of Service Vulnerability
<a href="#">CVE-2022-21888</a>	Windows Modern Execution Server Remote Code Execution Vulnerability
<a href="#">CVE-2022-21885</a>	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21884</a>	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21883</a>	Windows IKE Extension Denial of Service Vulnerability
<a href="#">CVE-2022-21882</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21881</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2022-21880</a>	Windows GDI+ Information Disclosure Vulnerability
<a href="#">CVE-2022-21874</a>	Windows Security Center API Remote Code Execution Vulnerability
<a href="#">CVE-2022-21843</a>	Windows IKE Extension Denial of Service Vulnerability
<a href="#">CVE-2022-2481</a>	Chromium: CVE-2022-2481 Use after free in Views
<a href="#">CVE-2022-2480</a>	Chromium: CVE-2022-2480 Use after free in Service Worker API
<a href="#">CVE-2022-2479</a>	Chromium: CVE-2022-2479 Insufficient validation of untrusted input in File
<a href="#">CVE-2022-2478</a>	Chromium: CVE-2022-2478 Use after free in PDF
<a href="#">CVE-2022-2477</a>	Chromium: CVE-2022-2477 Use after free in Guest View
<a href="#">CVE-2022-2295</a>	Chromium: CVE-2022-2295 Type Confusion in V8
<a href="#">CVE-2022-2294</a>	Chromium: CVE-2022-2294 Heap buffer overflow in WebRTC
<a href="#">CVE-2022-2165</a>	Chromium: CVE-2022-2165 Insufficient data validation in URL formatting
<a href="#">CVE-2022-2164</a>	Chromium: CVE-2022-2164 Inappropriate implementation in Extensions API
<a href="#">CVE-2022-2163</a>	Chromium: CVE-2022-2163 Use after free in Cast UI and Toolbar

<http://buildings.honeywell.com/security>

<a href="#">CVE-2022-2162</a>	Chromium: CVE-2022-2162 Insufficient policy enforcement in File System API
<a href="#">CVE-2022-2161</a>	Chromium: CVE-2022-2161 Use after free in WebApp Provider
<a href="#">CVE-2022-2160</a>	Chromium: CVE-2022-2160 Insufficient policy enforcement in DevTools
<a href="#">CVE-2022-2158</a>	Chromium: CVE-2022-2158 Type Confusion in V8
<a href="#">CVE-2022-2157</a>	Chromium: CVE-2022-2157 Use after free in Interest groups
<a href="#">CVE-2022-2156</a>	Chromium: CVE-2022-2156 Use after free in Base

## 2021 – Microsoft® Patches Tested with Pro-Watch

<a href="#">CVE-2021-43893</a>	Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43883</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43877</a>	ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43248</a>	Windows Digital Media Receiver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43247</a>	Windows TCP/IP Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43246</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-43245</a>	Windows Digital TV Tuner Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43244</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2021-43240</a>	NTFS Set Short Name Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43239</a>	Windows Recovery Environment Agent Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43238</a>	Windows Remote Access Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43237</a>	Windows Setup Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43236</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2021-43235</a>	Storage Spaces Controller Information Disclosure Vulnerability
<a href="#">CVE-2021-43234</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2021-43233</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2021-43232</a>	Windows Event Tracing Remote Code Execution Vulnerability
<a href="#">CVE-2021-43231</a>	Windows NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43230</a>	Windows NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43229</a>	Windows NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43228</a>	SymCrypt Denial of Service Vulnerability
<a href="#">CVE-2021-43227</a>	Storage Spaces Controller Information Disclosure Vulnerability
<a href="#">CVE-2021-43226</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43224</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-43223</a>	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2021-43222</a>	Microsoft Message Queuing Information Disclosure Vulnerability
<a href="#">CVE-2021-43219</a>	DirectX Graphics Kernel File Denial of Service Vulnerability
<a href="#">CVE-2021-43217</a>	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
<a href="#">CVE-2021-43216</a>	Microsoft Local Security Authority Server (lsasrv) Information Disclosure Vulnerability
<a href="#">CVE-2021-43215</a>	iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution
<a href="#">CVE-2021-43207</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42291</a>	Active Directory Domain Services Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42288</a>	Windows Hello Security Feature Bypass Vulnerability
<a href="#">CVE-2021-42287</a>	Active Directory Domain Services Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42285</a>	Windows Kernel Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-42284</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-42283</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42282</a>	Active Directory Domain Services Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42279</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2021-42278</a>	Active Directory Domain Services Elevation of Privilege Vulnerability
<a href="#">CVE-2021-42275</a>	Microsoft COM for Windows Remote Code Execution Vulnerability
<a href="#">CVE-2021-41367</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41361</a>	Active Directory Federation Server Spoofing Vulnerability
<a href="#">CVE-2021-41357</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41351</a>	Microsoft Edge (Chrome based) Spoofing on IE Mode
<a href="#">CVE-2021-41347</a>	Windows AppX Deployment Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41346</a>	Console Window Host Security Feature Bypass Vulnerability
<a href="#">CVE-2021-41345</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41343</a>	Windows Fast FAT File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-41342</a>	Windows MSHTML Platform Remote Code Execution Vulnerability
<a href="#">CVE-2021-41340</a>	Windows Graphics Component Remote Code Execution Vulnerability
<a href="#">CVE-2021-41339</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41338</a>	Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability
<a href="#">CVE-2021-41337</a>	Active Directory Security Feature Bypass Vulnerability
<a href="#">CVE-2021-41335</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41334</a>	Windows Desktop Bridge Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41333</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2021-41332</a>	Windows Print Spooler Information Disclosure Vulnerability
<a href="#">CVE-2021-41331</a>	Windows Media Audio Decoder Remote Code Execution Vulnerability
<a href="#">CVE-2021-41330</a>	Microsoft Windows Media Foundation Remote Code Execution Vulnerability
<a href="#">CVE-2021-40489</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40488</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40478</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40477</a>	Windows Event Tracing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40476</a>	Windows AppContainer Elevation Of Privilege Vulnerability
<a href="#">CVE-2021-40475</a>	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-40470</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40469</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2021-40468</a>	Windows Bind Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-40467</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40466</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40465</a>	Windows Text Shaping Remote Code Execution Vulnerability
<a href="#">CVE-2021-40464</a>	Windows Nearby Sharing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40463</a>	Windows NAT Denial of Service Vulnerability
<a href="#">CVE-2021-40462</a>	Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability
<a href="#">CVE-2021-40461</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2021-40460</a>	Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability
<a href="#">CVE-2021-40456</a>	Windows AD FS Security Feature Bypass Vulnerability
<a href="#">CVE-2021-40455</a>	Windows Installer Spoofing Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-40454</a>	Rich Text Edit Control Information Disclosure Vulnerability
<a href="#">CVE-2021-40450</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40449</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40447</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40443</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-40441</a>	Windows Media Center Elevation of Privilege Vulnerability
<a href="#">CVE-2021-38671</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2021-38667</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2021-38663</a>	Windows exFAT File System Information Disclosure Vulnerability
<a href="#">CVE-2021-38662</a>	Windows Fast FAT File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-38639</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-38638</a>	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
<a href="#">CVE-2021-38637</a>	Windows Storage Information Disclosure Vulnerability
<a href="#">CVE-2021-38624</a>	Windows Key Storage Provider Security Feature Bypass Vulnerability
<a href="#">CVE-2021-36970</a>	Windows Print Spooler Spoofing Vulnerability
<a href="#">CVE-2021-36967</a>	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-36965</a>	Windows WLAN AutoConfig Service Remote Code Execution Vulnerability
<a href="#">CVE-2021-36953</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2021-36948</a>	Windows Update Medic Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-36938</a>	Windows Cryptographic Primitives Library Information Disclosure Vulnerability
<a href="#">CVE-2021-36937</a>	Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability
<a href="#">CVE-2021-36936</a>	Windows Print Spooler Remote Code Execution Vulnerability
<a href="#">CVE-2021-36933</a>	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-36932</a>	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-36927</a>	Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability
<a href="#">CVE-2021-36926</a>	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-34456</a>	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34447</a>	Windows MSHTML Platform Remote Code Execution Vulnerability
<a href="#">CVE-2021-34500</a>	Windows Kernel Memory Information Disclosure Vulnerability
<a href="#">CVE-2021-34514</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34511</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34446</a>	Windows HTML Platforms Security Feature Bypass Vulnerability
<a href="#">CVE-2021-34496</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2021-34498</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34455</a>	Windows File History Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34494</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2021-34444</a>	Windows DNS Server Denial of Service Vulnerability
<a href="#">CVE-2021-34461</a>	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34492</a>	Windows Certificate Spoofing Vulnerability
<a href="#">CVE-2021-34459</a>	Windows AppContainer Elevation Of Privilege Vulnerability
<a href="#">CVE-2021-34504</a>	Windows Address Book Remote Code Execution Vulnerability
<a href="#">CVE-2021-34516</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34509</a>	Storage Spaces Controller Information Disclosure Vulnerability
<a href="#">CVE-2021-34513</a>	Storage Spaces Controller Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-34512</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-34448</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2021-34476</a>	Browser.sys Denial of Service Vulnerability
<a href="#">CVE-2021-33739</a>	Microsoft DWM Core Library Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31977</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-31976</a>	Server for NFS Information Disclosure Vulnerability
<a href="#">CVE-2021-31975</a>	Server for NFS Information Disclosure Vulnerability
<a href="#">CVE-2021-31974</a>	Server for NFS Denial of Service Vulnerability
<a href="#">CVE-2021-31973</a>	Windows GPSVC Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31972</a>	Event Tracing for Windows Information Disclosure Vulnerability
<a href="#">CVE-2021-31971</a>	Windows HTML Platform Security Feature Bypass Vulnerability
<a href="#">CVE-2021-31970</a>	Windows TCP/IP Driver Security Feature Bypass Vulnerability
<a href="#">CVE-2021-31959</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2021-31194</a>	OLE Automation Remote Code Execution Vulnerability
<a href="#">CVE-2021-31193</a>	Windows SSDP Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31191</a>	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-31190</a>	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31188</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31187</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-31186</a>	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
<a href="#">CVE-2021-28447</a>	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
<a href="#">CVE-2021-28446</a>	Windows Portmapping Information Disclosure Vulnerability
<a href="#">CVE-2021-28445</a>	Windows Network File System Remote Code Execution Vulnerability
<a href="#">CVE-2021-28444</a>	Windows Hyper-V Security Feature Bypass Vulnerability
<a href="#">CVE-2021-28443</a>	Windows Console Driver Denial of Service Vulnerability
<a href="#">CVE-2021-28442</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2021-28441</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2021-28440</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28439</a>	Windows TCP/IP Driver Denial of Service Vulnerability
<a href="#">CVE-2021-28438</a>	Windows Console Driver Denial of Service Vulnerability
<a href="#">CVE-2021-28437</a>	Windows Installer Information Disclosure Vulnerability
<a href="#">CVE-2021-28436</a>	Windows Speech Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28435</a>	Windows Event Tracing Information Disclosure Vulnerability
<a href="#">CVE-2021-28434</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28358</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28357</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28356</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28355</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28354</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28353</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28352</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28351</a>	Windows Speech Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28350</a>	Windows GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2021-28349</a>	Windows GDI+ Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-28348</a>	Windows GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2021-28347</a>	Windows Speech Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28346</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28345</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28344</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28343</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28342</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28341</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28340</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28339</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28338</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28337</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28336</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28335</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28334</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28333</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28332</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28331</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28330</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28329</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28328</a>	Windows DNS Information Disclosure Vulnerability
<a href="#">CVE-2021-28327</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-28326</a>	Windows AppX Deployment Server Denial of Service Vulnerability
<a href="#">CVE-2021-28325</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2021-28324</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2021-28323</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2021-28322</a>	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28321</a>	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28320</a>	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28319</a>	Windows TCP/IP Driver Denial of Service Vulnerability
<a href="#">CVE-2021-28318</a>	Windows GDI+ Information Disclosure Vulnerability
<a href="#">CVE-2021-28317</a>	Microsoft Windows Codecs Library Information Disclosure Vulnerability
<a href="#">CVE-2021-28316</a>	Microsoft Windows Codecs Library Information Disclosure Vulnerability
<a href="#">CVE-2021-28315</a>	Windows Media Video Decoder Remote Code Execution Vulnerability
<a href="#">CVE-2021-28314</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28313</a>	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28312</a>	Windows NTFS Denial of Service Vulnerability
<a href="#">CVE-2021-28311</a>	Windows Application Compatibility Cache Denial of Service Vulnerability
<a href="#">CVE-2021-28310</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-28309</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2021-27096</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2021-27095</a>	Windows Media Video Decoder Remote Code Execution Vulnerability
<a href="#">CVE-2021-27094</a>	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
<a href="#">CVE-2021-27093</a>	Windows Kernel Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-27092</a>	Azure AD Web Sign-in Security Feature Bypass Vulnerability
<a href="#">CVE-2021-27090</a>	Windows Secure Kernel Mode Elevation of Privilege Vulnerability
<a href="#">CVE-2021-27089</a>	Microsoft Internet Messaging API Remote Code Execution Vulnerability
<a href="#">CVE-2021-27088</a>	Windows Event Tracing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-27086</a>	Windows Services and Controller App Elevation of Privilege Vulnerability
<a href="#">CVE-2021-27079</a>	Windows Media Photo Codec Information Disclosure Vulnerability
<a href="#">CVE-2021-27072</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-26442</a>	Windows HTTP.sys Elevation of Privilege Vulnerability
<a href="#">CVE-2021-26441</a>	Storage Spaces Controller Elevation of Privilege Vulnerability
<a href="#">CVE-2021-26435</a>	Windows Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2021-26433</a>	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-26432</a>	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability
<a href="#">CVE-2021-26426</a>	Windows User Account Profile Picture Elevation of Privilege Vulnerability
<a href="#">CVE-2021-26424</a>	Windows TCP/IP Remote Code Execution Vulnerability
<a href="#">CVE-2021-26419</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2021-26417</a>	Windows Overlay Filter Information Disclosure Vulnerability
<a href="#">CVE-2021-26416</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-26415</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE 2021 26414</a>	Windows DCOM Server Security Feature Bypass
<a href="#">CVE-2021-26413</a>	Windows Installer Spoofing Vulnerability
<a href="#">CVE-2021-24111</a>	.NET Framework Denial of Service Vulnerability
<a href="#">CVE-2021-24103</a>	Windows Event Tracing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-24102</a>	Windows Event Tracing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-24098</a>	Windows Console Driver Denial of Service Vulnerability
<a href="#">CVE-2021-24086</a>	Windows TCP/IP Denial of Service Vulnerability
<a href="#">CVE-2021-24082</a>	Microsoft.PowerShell.Utility Module WDAC Security Feature Bypass Vulnerability
<a href="#">CVE-2021-24081</a>	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
<a href="#">CVE-2021-24076</a>	Microsoft Windows VMSwitch Information Disclosure Vulnerability
<a href="#">CVE-2021-24075</a>	Windows Network File System Denial of Service Vulnerability
<a href="#">CVE-2021-24106</a>	Windows DirectX Information Disclosure Vulnerability
<a href="#">CVE-2021-24096</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2021-24094</a>	Windows TCP/IP Remote Code Execution Vulnerability
<a href="#">CVE-2021-24093</a>	Windows Graphics Component Remote Code Execution Vulnerability
<a href="#">CVE-2021-24091</a>	Windows Camera Codec Pack Remote Code Execution Vulnerability
<a href="#">CVE-2021-24088</a>	Windows Local Spooler Remote Code Execution Vulnerability
<a href="#">CVE-2021-25195</a>	Windows PKU2U Elevation of Privilege Vulnerability
<a href="#">CVE-2021-24084</a>	Windows Mobile Device Management Information Disclosure Vulnerability
<a href="#">CVE-2021-24083</a>	Windows Address Book Remote Code Execution Vulnerability
<a href="#">CVE-2021-24080</a>	Windows Trust Verification API Denial of Service Vulnerability
<a href="#">CVE-2021-24079</a>	Windows Backup Engine Information Disclosure Vulnerability
<a href="#">CVE-2021-24078</a>	Windows DNS Server Remote Code Execution Vulnerability
<a href="#">CVE-2021-24077</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2021-24074</a>	Windows TCP/IP Remote Code Execution Vulnerability
<a href="#">CVE-2021-1734</a>	Windows Remote Procedure Call Information Disclosure Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-1732</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1731</a>	PFX Encryption Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1727</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1722</a>	Windows Fax Service Remote Code Execution Vulnerability
<a href="#">CVE-2021-1710</a>	Microsoft Windows Media Foundation Remote Code Execution Vulnerability
<a href="#">CVE-2021-1709</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1708</a>	Windows GDI+ Information Disclosure Vulnerability
<a href="#">CVE-2021-1706</a>	Windows LUAfv Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1705</a>	Microsoft Edge (HTML-based) Memory Corruption Vulnerability
<a href="#">CVE-2021-1704</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1703</a>	Windows Event Logging Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1702</a>	Windows Remote Procedure Call Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1701</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1700</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1699</a>	Windows (modem.sys) Information Disclosure Vulnerability
<a href="#">CVE-2021-1698</a>	Windows Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1697</a>	Windows InstallService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1696</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2021-1695</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1694</a>	Windows Update Stack Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1693</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1692</a>	Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-1691</a>	Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2021-1690</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1689</a>	Windows Multipoint Management Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1688</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1687</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1686</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1685</a>	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1684</a>	Windows Bluetooth Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1683</a>	Windows Bluetooth Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1682</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1681</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1680</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1679</a>	Windows CryptoAPI Denial of Service Vulnerability
<a href="#">CVE-2021-1678</a>	NTLM Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1676</a>	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-1674</a>	Windows Remote Desktop Protocol Core Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1673</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1672</a>	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-1671</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1670</a>	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-1669</a>	Windows Remote Desktop Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1668</a>	Microsoft DTV-DVD Video Decoder Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2021-1667</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1666</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1665</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2021-1664</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1663</a>	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-1662</a>	Windows Event Tracing Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1661</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1660</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1659</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1658</a>	Remote Procedure Call Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2021-1657</a>	Windows Fax Compose Form Remote Code Execution Vulnerability
<a href="#">CVE-2021-1656</a>	TPM Device Driver Information Disclosure Vulnerability
<a href="#">CVE-2021-1655</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1654</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1653</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1652</a>	Windows CSC Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1651</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1650</a>	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1649</a>	Active Template Library Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1648</a>	Microsoft splwow64 Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1646</a>	Windows WLAN Service Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1645</a>	Windows Docker Information Disclosure Vulnerability
<a href="#">CVE-2021-1642</a>	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1640</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2021-1638</a>	Windows Bluetooth Security Feature Bypass Vulnerability
<a href="#">CVE-2021-1637</a>	Windows DNS Query Information Disclosure Vulnerability
<a href="#">CVE-2021-1636</a>	Microsoft SQL Elevation of Privilege Vulnerability

## 2020 – Microsoft® Patches Tested with Pro-Watch

<a href="#">CVE-2020-24588</a>	Windows Wireless Networking Spoofing Vulnerability
<a href="#">CVE-2020-17140</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2020-17139</a>	Windows Overlay Filter Security Feature Bypass Vulnerability
<a href="#">CVE-2020-17138</a>	Windows Error Reporting Information Disclosure Vulnerability
<a href="#">CVE-2020-17137</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-17136</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2020-17134</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2020-17131</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-17113</a>	Windows Camera Codec Information Disclosure Vulnerability
<a href="#">CVE-2020-17103</a>	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2020-17099</a>	Windows Lock Screen Security Feature Bypass Vulnerability
<a href="#">CVE-2020-17098</a>	Windows GDI+ Information Disclosure Vulnerability
<a href="#">CVE-2020-17097</a>	Windows Digital Media Receiver Elevation of Privilege Vulnerability
<a href="#">CVE-2020-17096</a>	Windows NTFS Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-17095	Hyper-V Remote Code Execution Vulnerability
CVE-2020-17094	Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-17092	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-17090	Microsoft Defender for Endpoint Security Feature Bypass Vulnerability
CVE-2020-17088	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-17088	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-17087	Windows Kernel Local Elevation of Privilege Vulnerability
CVE-2020-17087	Windows Kernel Local Elevation of Privilege Vulnerability
CVE-2020-17077	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-17076	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17075	Windows USO Core Worker Elevation of Privilege Vulnerability
CVE-2020-17074	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17073	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17071	Windows Delivery Optimization Information Disclosure Vulnerability
CVE-2020-17070	Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2020-17069	Windows NDIS Information Disclosure Vulnerability
CVE-2020-17069	Windows NDIS Information Disclosure Vulnerability
CVE-2020-17068	Windows GDI+ Remote Code Execution Vulnerability
CVE-2020-17068	Windows GDI+ Remote Code Execution Vulnerability
CVE-2020-17058	Microsoft Browser Memory Corruption Vulnerability
CVE-2020-17057	Windows Win32k Elevation of Privilege Vulnerability
CVE-2020-17056	Windows Network File System Information Disclosure Vulnerability
CVE-2020-17056	Windows Network File System Information Disclosure Vulnerability
CVE-2020-17055	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17055	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17054	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2020-17053	Internet Explorer Memory Corruption Vulnerability
CVE-2020-17052	Scripting Engine Memory Corruption Vulnerability
CVE-2020-17052	Scripting Engine Memory Corruption Vulnerability
CVE-2020-17051	Windows Network File System Remote Code Execution Vulnerability
CVE-2020-17051	Windows Network File System Remote Code Execution Vulnerability
CVE-2020-17049	Kerberos KDC Security Feature Bypass Vulnerability
CVE-2020-17049	Kerberos KDC Security Feature Bypass Vulnerability
CVE-2020-17048	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2020-17047	Windows Network File System Denial of Service Vulnerability
CVE-2020-17047	Windows Network File System Denial of Service Vulnerability
CVE-2020-17046	Windows Error Reporting Denial of Service Vulnerability
CVE-2020-17045	Windows KernelStream Information Disclosure Vulnerability
CVE-2020-17045	Windows KernelStream Information Disclosure Vulnerability
CVE-2020-17044	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17044	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17043	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17043	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17042	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2020-17042	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2020-17041	Windows Print Configuration Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-17041	Windows Print Configuration Elevation of Privilege Vulnerability
CVE-2020-17040	Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2020-17040	Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2020-17038	Win32k Elevation of Privilege Vulnerability
CVE-2020-17038	Win32k Elevation of Privilege Vulnerability
CVE-2020-17037	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-17036	Windows Function Discovery SSDP Provider Information Disclosure Vulnerability
CVE-2020-17036	Windows Function Discovery SSDP Provider Information Disclosure Vulnerability
CVE-2020-17035	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-17034	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17034	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17033	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17033	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17032	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17032	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17031	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17031	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17030	Windows MSCTF Server Information Disclosure Vulnerability
CVE-2020-17029	Windows Canonical Display Driver Information Disclosure Vulnerability
CVE-2020-17029	Windows Canonical Display Driver Information Disclosure Vulnerability
CVE-2020-17028	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17028	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17027	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17027	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17026	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17026	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17025	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17025	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17024	Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability
CVE-2020-17024	Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability
CVE-2020-17014	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17014	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17013	Win32k Information Disclosure Vulnerability
CVE-2020-17011	Windows Port Class Library Elevation of Privilege Vulnerability
CVE-2020-17011	Windows Port Class Library Elevation of Privilege Vulnerability
CVE-2020-17010	Win32k Elevation of Privilege Vulnerability
CVE-2020-17007	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-17004	Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-17004	Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-17001	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17001	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17000	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2020-17000	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2020-16999	Windows WalletService Information Disclosure Vulnerability
CVE-2020-16998	DirectX Elevation of Privilege Vulnerability
CVE-2020-16997	Remote Desktop Protocol Server Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-16997	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2020-16996	Kerberos Security Feature Bypass Vulnerability
CVE-2020-16980	Windows iSCSI Target Service Elevation of Privilege Vulnerability
CVE-2020-16976	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16975	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16974	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16973	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16972	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16968	Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-16967	Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-16964	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16963	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16962	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16961	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16960	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16959	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16958	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16940	Windows - User Profile Service Elevation of Privilege Vulnerability
CVE-2020-16939	Group Policy Elevation of Privilege Vulnerability
CVE-2020-16938	Windows Kernel Information Disclosure Vulnerability
CVE-2020-16937	.NET Framework Information Disclosure Vulnerability
CVE-2020-16936	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16935	Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-16927	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2020-16924	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-16923	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-16922	Windows Spoofing Vulnerability
CVE-2020-16921	Windows Text Services Framework Information Disclosure Vulnerability
CVE-2020-16920	Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
CVE-2020-16919	Windows Enterprise App Management Service Information Disclosure Vulnerability
CVE-2020-16916	Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-16915	Media Foundation Memory Corruption Vulnerability
CVE-2020-16914	Windows GDI+ Information Disclosure Vulnerability
CVE-2020-16913	Win32k Elevation of Privilege Vulnerability
CVE-2020-16912	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16911	GDI+ Remote Code Execution Vulnerability
CVE-2020-16910	Windows Security Feature Bypass Vulnerability
CVE-2020-16909	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-16907	Win32k Elevation of Privilege Vulnerability
CVE-2020-16905	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-16902	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-16900	Windows Event System Elevation of Privilege Vulnerability
CVE-2020-16899	Windows TCP/IP Denial of Service Vulnerability
CVE-2020-16898	Windows TCP/IP Remote Code Execution Vulnerability
CVE-2020-16897	NetBT Information Disclosure Vulnerability
CVE-2020-16896	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-16895	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-16894	Windows NAT Denial of Service Vulnerability
CVE-2020-16892	Windows Image Elevation of Privilege Vulnerability
CVE-2020-16891	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2020-16890	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-16889	Windows KernelStream Information Disclosure Vulnerability
CVE-2020-16887	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-16885	Windows Storage VSP Driver Elevation of Privilege Vulnerability
CVE-2020-16879	Projected Filesystem Information Disclosure Vulnerability
CVE-2020-16877	Windows Elevation of Privilege Vulnerability
CVE-2020-16876	Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
CVE-2020-16854	Windows Kernel Information Disclosure Vulnerability
CVE-2020-8927	Brotli Library Buffer Overflow Vulnerability
CVE-2020-1599	Windows Spoofing Vulnerability
CVE-2020-1599	Windows Spoofing Vulnerability
CVE-2020-1598	Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-1596	TLS Information Disclosure Vulnerability
CVE-2020-1593	Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2020-1592	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1590	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-1589	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1587	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2020-1584	Windows dnssrvr.dll Elevation of Privilege Vulnerability
CVE-2020-1579	Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability
CVE-2020-1578	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1577	DirectWrite Information Disclosure Vulnerability
CVE-2020-1570	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1569	Microsoft Edge Memory Corruption Vulnerability
CVE-2020-1568	Microsoft Edge PDF Remote Code Execution Vulnerability
CVE-2020-1567	MSHTML Engine Remote Code Execution Vulnerability
CVE-2020-1566	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1565	Windows Elevation of Privilege Vulnerability
CVE-2020-1564	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1562	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1561	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1559	Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-1558	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1557	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1556	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1555	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1554	Media Foundation Memory Corruption Vulnerability
CVE-2020-1553	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1552	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-1551	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1550	Windows CDP User Components Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1549	Windows CDP User Components Elevation of Privilege Vulnerability
CVE-2020-1548	Windows WaasMedic Service Information Disclosure Vulnerability
CVE-2020-1547	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1546	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1545	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1544	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1543	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1542	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1541	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1540	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1539	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1538	Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1537	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-1536	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1535	Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1534	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-1533	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1532	Windows InstallService Elevation of Privilege Vulnerability
CVE-2020-1531	Windows Accounts Control Elevation of Privilege Vulnerability
CVE-2020-1530	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-1529	Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1528	Windows Radio Manager API Elevation of Privilege Vulnerability
CVE-2020-1527	Windows Custom Protocol Engine Elevation of Privilege Vulnerability
CVE-2020-1526	Windows Network Connection Broker Elevation of Privilege Vulnerability
CVE-2020-1525	Media Foundation Memory Corruption Vulnerability
CVE-2020-1524	Windows Speech Shell Components Elevation of Privilege Vulnerability
CVE-2020-1522	Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2020-1521	Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2020-1520	Windows Font Driver Host Remote Code Execution Vulnerability
CVE-2020-1519	Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1518	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1517	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1516	Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1515	Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2020-1513	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-1512	Windows State Repository Service Information Disclosure Vulnerability
CVE-2020-1511	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-1510	Win32k Information Disclosure Vulnerability
CVE-2020-1509	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2020-1508	Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2020-1507	Microsoft COM for Windows Elevation of Privilege Vulnerability
CVE-2020-1506	Windows Start-Up Application Elevation of Privilege Vulnerability
CVE-2020-1492	Media Foundation Memory Corruption Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1491	Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-1490	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2020-1489	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-1488	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2020-1487	Media Foundation Information Disclosure Vulnerability
CVE-2020-1486	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1485	Windows Image Acquisition Service Information Disclosure Vulnerability
CVE-2020-1484	Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1480	Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1479	DirectX Elevation of Privilege Vulnerability
CVE-2020-1478	Media Foundation Memory Corruption Vulnerability
CVE-2020-1477	Media Foundation Memory Corruption Vulnerability
CVE-2020-1476	ASP.NET and .NET Elevation of Privilege Vulnerability
CVE-2020-1475	Windows Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1474	Windows Image Acquisition Service Information Disclosure Vulnerability
CVE-2020-1473	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1472	Netlogon Elevation of Privilege Vulnerability
CVE-2020-1471	Windows CloudExperienceHost Elevation of Privilege Vulnerability
CVE-2020-1470	Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1468	Windows GDI Information Disclosure Vulnerability
CVE-2020-1467	Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-1466	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2020-1464	Windows Spoofing Vulnerability
CVE-2020-1463	Windows SharedStream Library Elevation of Privilege Vulnerability
CVE-2020-1462	Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability
CVE-2020-1459	Windows ARM Information Disclosure Vulnerability
CVE-2020-1441	Windows Spatial Data Service Elevation of Privilege Vulnerability
CVE-2020-1438	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1437	Windows Network Location Awareness Service Elevation of Privilege Vulnerability
CVE-2020-1436	Windows Font Library Remote Code Execution Vulnerability
CVE-2020-1435	GDI+ Remote Code Execution Vulnerability
CVE-2020-1434	Windows Sync Host Service Elevation of Privilege Vulnerability
CVE-2020-1433	Microsoft Edge PDF Information Disclosure Vulnerability
CVE-2020-1432	Skype for Business via Internet Explorer Information Disclosure Vulnerability
CVE-2020-1431	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2020-1430	Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1429	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-1428	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1427	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1426	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1424	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-1422	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1421	LNK Remote Code Execution Vulnerability
CVE-2020-1420	Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-1419	Windows Kernel Information Disclosure Vulnerability



<http://buildings.honeywell.com/security>

CVE-2020-1418	Windows Diagnostics Hub Elevation of Privilege Vulnerability
CVE-2020-1417	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1415	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1414	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1413	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1412	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1411	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1410	Windows Address Book Remote Code Execution Vulnerability
CVE-2020-1409	DirectWrite Remote Code Execution Vulnerability
CVE-2020-1408	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2020-1407	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1406	Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-1405	Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-1404	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1403	VBScript Remote Code Execution Vulnerability
CVE-2020-1402	Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-1401	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1400	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1399	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1398	Windows Lockscreen Elevation of Privilege Vulnerability
CVE-2020-1397	Windows Imaging Component Information Disclosure Vulnerability
CVE-2020-1396	Windows ALPC Elevation of Privilege Vulnerability
CVE-2020-1395	Windows Elevation of Privilege Vulnerability
CVE-2020-1394	Windows Elevation of Privilege Vulnerability
CVE-2020-1393	Windows Diagnostics Hub Elevation of Privilege Vulnerability
CVE-2020-1392	Windows Elevation of Privilege Vulnerability
CVE-2020-1391	Windows Agent Activation Runtime Information Disclosure Vulnerability
CVE-2020-1390	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1389	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1388	Windows Elevation of Privilege Vulnerability
CVE-2020-1387	Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1386	Connected User Experiences and Telemetry Service Information Disclosure Vulnerability
CVE-2020-1385	Windows Credential Picker Elevation of Privilege Vulnerability
CVE-2020-1384	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2020-1383	Windows RRAS Service Information Disclosure Vulnerability
CVE-2020-1382	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1381	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1380	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1379	Media Foundation Memory Corruption Vulnerability
CVE-2020-1378	Windows Registry Elevation of Privilege Vulnerability
CVE-2020-1377	Windows Registry Elevation of Privilege Vulnerability
CVE-2020-1376	Windows Elevation of Privilege Vulnerability
CVE-2020-1375	Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-1374	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-1373	Windows Network Connections Service Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1372	Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-1371	Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2020-1370	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1369	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1368	Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability
CVE-2020-1367	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1366	Windows Print Workflow Service Elevation of Privilege Vulnerability
CVE-2020-1365	Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2020-1364	Windows WalletService Denial of Service Vulnerability
CVE-2020-1363	Windows Picker Platform Elevation of Privilege Vulnerability
CVE-2020-1362	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1361	Windows WalletService Information Disclosure Vulnerability
CVE-2020-1360	Windows Profile Service Elevation of Privilege Vulnerability
CVE-2020-1359	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2020-1358	Windows Resource Policy Information Disclosure Vulnerability
CVE-2020-1357	Windows System Events Broker Elevation of Privilege Vulnerability
CVE-2020-1356	Windows iSCSI Target Service Elevation of Privilege Vulnerability
CVE-2020-1355	Windows Font Driver Host Remote Code Execution Vulnerability
CVE-2020-1354	Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1353	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1352	Windows USO Core Worker Elevation of Privilege Vulnerability
CVE-2020-1351	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1350	Windows DNS Server Remote Code Execution Vulnerability
CVE-2020-1348	Windows GDI Information Disclosure Vulnerability
CVE-2020-1347	Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-1346	Windows Modules Installer Elevation of Privilege Vulnerability
CVE-2020-1344	Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1339	Windows Media Remote Code Execution Vulnerability
CVE-2020-1337	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-1336	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1334	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1333	Group Policy Services Policy Processing Elevation of Privilege Vulnerability
CVE-2020-1330	Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability
CVE-2020-1324	Windows Elevation of Privilege Vulnerability
CVE-2020-1317	Group Policy Elevation of Privilege Vulnerability
CVE-2020-1316	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1315	Internet Explorer Information Disclosure Vulnerability
CVE-2020-1314	Windows Text Service Framework Elevation of Privilege Vulnerability
CVE-2020-1313	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-1312	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1311	Component Object Model Elevation of Privilege Vulnerability
CVE-2020-1310	Win32k Elevation of Privilege Vulnerability
CVE-2020-1309	Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1308	DirectX Elevation of Privilege Vulnerability
CVE-2020-1307	Windows Kernel Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2020-1306</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1305</a>	Windows State Repository Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1304</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1303</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1302</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1301</a>	Windows SMB Authenticated Remote Code Execution Vulnerability
<a href="#">CVE-2020-1300</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2020-1299</a>	LNK Remote Code Execution Vulnerability
<a href="#">CVE-2020-1296</a>	Windows Diagnostics & feedback Information Disclosure Vulnerability
<a href="#">CVE-2020-1294</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1293</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1292</a>	OpenSSH for Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1291</a>	Windows Network Connections Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1290</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2020-1287</a>	Windows WalletService Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1286</a>	Windows Shell Remote Code Execution Vulnerability
<a href="#">CVE-2020-1285</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2020-1283</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2020-1282</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1281</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2020-1280</a>	Windows Bluetooth Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1279</a>	Windows Lockscreen Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1278</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1277</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1276</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1275</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1274</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1273</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1272</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1271</a>	Windows Backup Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1270</a>	Windows WLAN Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1269</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1268</a>	Windows Service Information Disclosure Vulnerability
<a href="#">CVE-2020-1267</a>	Local Security Authority Subsystem Service Denial of Service Vulnerability
<a href="#">CVE-2020-1266</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1265</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1264</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1263</a>	Windows Error Reporting Information Disclosure Vulnerability
<a href="#">CVE-2020-1262</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1261</a>	Windows Error Reporting Information Disclosure Vulnerability
<a href="#">CVE-2020-1260</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-1259</a>	Windows Host Guardian Service Security Feature Bypass Vulnerability
<a href="#">CVE-2020-1258</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1257</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1256</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2020-1255</a>	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1254	Windows Modules Installer Service Elevation of Privilege Vulnerability
CVE-2020-1253	Win32k Elevation of Privilege Vulnerability
CVE-2020-1252	Windows Remote Code Execution Vulnerability
CVE-2020-1251	Win32k Elevation of Privilege Vulnerability
CVE-2020-1250	Win32k Information Disclosure Vulnerability
CVE-2020-1249	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1248	GDI+ Remote Code Execution Vulnerability
CVE-2020-1247	Win32k Elevation of Privilege Vulnerability
CVE-2020-1246	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1245	Win32k Elevation of Privilege Vulnerability
CVE-2020-1244	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1243	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-1242	Microsoft Edge Information Disclosure Vulnerability
CVE-2020-1241	Windows Kernel Security Feature Bypass Vulnerability
CVE-2020-1239	Media Foundation Memory Corruption Vulnerability
CVE-2020-1238	Media Foundation Memory Corruption Vulnerability
CVE-2020-1237	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1236	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1235	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1234	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1233	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1232	Media Foundation Information Disclosure Vulnerability
CVE-2020-1231	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1230	VBScript Remote Code Execution Vulnerability
CVE-2020-1228	Windows DNS Denial of Service Vulnerability
CVE-2020-1222	Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1220	Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability
CVE-2020-1219	Microsoft Browser Memory Corruption Vulnerability
CVE-2020-1217	Windows Runtime Information Disclosure Vulnerability
CVE-2020-1216	VBScript Remote Code Execution Vulnerability
CVE-2020-1215	VBScript Remote Code Execution Vulnerability
CVE-2020-1214	VBScript Remote Code Execution Vulnerability
CVE-2020-1213	VBScript Remote Code Execution Vulnerability
CVE-2020-1212	OLE Automation Elevation of Privilege Vulnerability
CVE-2020-1211	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-1209	Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-1208	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1207	Win32k Elevation of Privilege Vulnerability
CVE-2020-1206	Windows SMBv3 Client/Server Information Disclosure Vulnerability
CVE-2020-1204	Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-1203	Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1202	Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1201	Windows Now Playing Session Manager Elevation of Privilege Vulnerability
CVE-2020-1199	Windows Feedback Hub Elevation of Privilege Vulnerability
CVE-2020-1197	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-1196	Windows Print Configuration Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1194	Windows Registry Denial of Service Vulnerability
CVE-2020-1191	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1190	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1189	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1188	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1187	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1186	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1185	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1184	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1180	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1179	Windows GDI Information Disclosure Vulnerability
CVE-2020-1176	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1175	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1174	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1172	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1169	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1167	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1166	Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1165	Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1164	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1162	Windows Elevation of Privilege Vulnerability
CVE-2020-1160	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1159	Windows Elevation of Privilege Vulnerability
CVE-2020-1158	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1157	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1156	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1155	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1154	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-1153	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1152	Windows Win32k Elevation of Privilege Vulnerability
CVE-2020-1151	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1149	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1147	.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability
CVE-2020-1147	.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability
CVE-2020-1146	Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1145	Windows GDI Information Disclosure Vulnerability
CVE-2020-1144	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1143	Win32k Elevation of Privilege Vulnerability
CVE-2020-1142	Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1141	Windows GDI Information Disclosure Vulnerability
CVE-2020-1140	DirectX Elevation of Privilege Vulnerability
CVE-2020-1139	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1138	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2020-1137	Windows Push Notification Service Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2020-1136</a>	Media Foundation Memory Corruption Vulnerability
<a href="#">CVE-2020-1135</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1134</a>	Windows State Repository Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1133</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1132</a>	Windows Error Reporting Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1131</a>	Windows State Repository Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1130</a>	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1129</a>	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
<a href="#">CVE-2020-1126</a>	Media Foundation Memory Corruption Vulnerability
<a href="#">CVE-2020-1125</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1124</a>	Windows State Repository Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1123</a>	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
<a href="#">CVE-2020-1122</a>	Windows Language Pack Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1121</a>	Windows Clipboard Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1119</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2020-1118</a>	Microsoft Windows Transport Layer Security Denial of Service Vulnerability
<a href="#">CVE-2020-1117</a>	Microsoft Color Management Remote Code Execution Vulnerability
<a href="#">CVE-2020-1116</a>	Windows CSRSS Information Disclosure Vulnerability
<a href="#">CVE-2020-1115</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1114</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1113</a>	Windows Task Scheduler Security Feature Bypass Vulnerability
<a href="#">CVE-2020-1112</a>	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1111</a>	Windows Clipboard Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1110</a>	Windows Update Stack Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1109</a>	Windows Update Stack Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1108</a>	.NET Core & .NET Framework Denial of Service Vulnerability
<a href="#">CVE-2020-1098</a>	Windows Shell Infrastructure Component Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1097</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2020-1096</a>	Microsoft Edge PDF Remote Code Execution Vulnerability
<a href="#">CVE-2020-1094</a>	Windows Work Folder Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1093</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-1092</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2020-1091</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2020-1090</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1088</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1087</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1086</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1085</a>	Windows Function Discovery Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1084</a>	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
<a href="#">CVE-2020-1083</a>	Microsoft Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2020-1082</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1081</a>	Windows Printer Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1080</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1079</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1078</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1077</a>	Windows Runtime Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2020-1076</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2020-1075</a>	Windows Subsystem for Linux Information Disclosure Vulnerability
<a href="#">CVE-2020-1074</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2020-1073</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-1072</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2020-1071</a>	Windows Remote Access Common Dialog Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1070</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1068</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1067</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2020-1065</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-1064</a>	MSHTML Engine Remote Code Execution Vulnerability
<a href="#">CVE-2020-1062</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2020-1061</a>	Microsoft Script Runtime Remote Code Execution Vulnerability
<a href="#">CVE-2020-1060</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-1059</a>	Microsoft Edge Spoofing Vulnerability
<a href="#">CVE-2020-1058</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-1057</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-1056</a>	Microsoft Edge Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1055</a>	Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability
<a href="#">CVE-2020-1054</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1053</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1052</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1051</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2020-1048</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1047</a>	Windows Hyper-V Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1046</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2020-1039</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2020-1038</a>	Windows Routing Utilities Denial of Service
<a href="#">CVE-2020-1037</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-1035</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-1034</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1033</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2020-1031</a>	Windows DHCP Server Information Disclosure Vulnerability
<a href="#">CVE-2020-1030</a>	Windows Print Spooler Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1029</a>	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1028</a>	Media Foundation Memory Corruption Vulnerability
<a href="#">CVE-2020-1027</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1021</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1020</a>	Adobe Font Manager Library Remote Code Execution Vulnerability
<a href="#">CVE-2020-1017</a>	Windows Push Notification Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1016</a>	Windows Push Notification Service Information Disclosure Vulnerability
<a href="#">CVE-2020-1015</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1014</a>	Microsoft Windows Update Client Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1013</a>	Group Policy Elevation of Privilege Vulnerability
<a href="#">CVE-2020-1012</a>	WinINet API Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-1011	Windows Elevation of Privilege Vulnerability
CVE-2020-1010	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-1009	Windows Elevation of Privilege Vulnerability
CVE-2020-1008	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1007	Windows Kernel Information Disclosure Vulnerability
CVE-2020-1006	Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1005	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1004	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1003	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1001	Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1000	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0999	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0998	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0997	Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-0996	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-0995	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0994	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0993	Windows DNS Denial of Service Vulnerability
CVE-2020-0992	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0989	Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability
CVE-2020-0988	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0987	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0986	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0985	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-0983	Windows Elevation of Privilege Vulnerability
CVE-2020-0982	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0981	Windows Token Security Feature Bypass Vulnerability
CVE-2020-0970	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0969	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2020-0968	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0967	VBScript Remote Code Execution Vulnerability
CVE-2020-0966	VBScript Remote Code Execution Vulnerability
CVE-2020-0965	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-0964	GDI+ Remote Code Execution Vulnerability
CVE-2020-0963	Windows GDI Information Disclosure Vulnerability
CVE-2020-0962	Win32k Information Disclosure Vulnerability
CVE-2020-0960	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0959	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0958	Win32k Elevation of Privilege Vulnerability
CVE-2020-0956	Win32k Elevation of Privilege Vulnerability
CVE-2020-0955	Windows Kernel Information Disclosure in CPU Memory Access
CVE-2020-0953	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0952	Windows GDI Information Disclosure Vulnerability
CVE-2020-0951	Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2020-0950	Media Foundation Memory Corruption Vulnerability



<http://buildings.honeywell.com/security>

CVE-2020-0949	Media Foundation Memory Corruption Vulnerability
CVE-2020-0948	Media Foundation Memory Corruption Vulnerability
CVE-2020-0947	Media Foundation Information Disclosure Vulnerability
CVE-2020-0946	Media Foundation Information Disclosure Vulnerability
CVE-2020-0945	Media Foundation Information Disclosure Vulnerability
CVE-2020-0944	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0942	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0941	Win32k Information Disclosure Vulnerability
CVE-2020-0940	Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-0939	Media Foundation Information Disclosure Vulnerability
CVE-2020-0938	Adobe Font Manager Library Remote Code Execution Vulnerability
CVE-2020-0937	Media Foundation Information Disclosure Vulnerability
CVE-2020-0936	Windows Scheduled Task Elevation of Privilege Vulnerability
CVE-2020-0934	Windows Elevation of Privilege Vulnerability
CVE-2020-0928	Windows Kernel Information Disclosure Vulnerability
CVE-2020-0922	Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2020-0921	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0918	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-0917	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-0916	Windows GDI Elevation of Privilege Vulnerability
CVE-2020-0915	Windows GDI Elevation of Privilege Vulnerability
CVE-2020-0914	Windows State Repository Service Information Disclosure Vulnerability
CVE-2020-0913	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0912	Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability
CVE-2020-0911	Windows Modules Installer Elevation of Privilege Vulnerability
CVE-2020-0910	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2020-0909	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0908	Windows Text Service Module Remote Code Execution Vulnerability
CVE-2020-0907	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-0904	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0897	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0896	Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0895	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2020-0890	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0889	Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0888	DirectX Elevation of Privilege Vulnerability
CVE-2020-0887	Win32k Elevation of Privilege Vulnerability
CVE-2020-0886	Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-0885	Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-0883	GDI+ Remote Code Execution Vulnerability
CVE-2020-0882	Windows GDI Information Disclosure Vulnerability
CVE-2020-0881	GDI+ Remote Code Execution Vulnerability
CVE-2020-0880	Windows GDI Information Disclosure Vulnerability
CVE-2020-0879	Windows GDI Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2020-0878</a>	Microsoft Browser Memory Corruption Vulnerability
<a href="#">CVE-2020-0877</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0876</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2020-0875</a>	Microsoft splwow64 Information Disclosure Vulnerability
<a href="#">CVE-2020-0874</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2020-0871</a>	Windows Network Connections Service Information Disclosure Vulnerability
<a href="#">CVE-2020-0870</a>	Shell infrastructure component Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0869</a>	Media Foundation Memory Corruption Vulnerability
<a href="#">CVE-2020-0868</a>	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0867</a>	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0866</a>	Windows Work Folder Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0865</a>	Windows Work Folder Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0864</a>	Windows Work Folder Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0863</a>	Connected User Experiences and Telemetry Service Information Disclosure Vulnerability
<a href="#">CVE-2020-0861</a>	Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability
<a href="#">CVE-2020-0860</a>	Windows ActiveX Installer Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0859</a>	Windows Modules Installer Service Information Disclosure Vulnerability
<a href="#">CVE-2020-0858</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0857</a>	Windows Search Indexer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0856</a>	Active Directory Information Disclosure Vulnerability
<a href="#">CVE-2020-0854</a>	Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0853</a>	CVE-2020-0853   Windows Imaging Component Information Disclosure Vulnerability
<a href="#">CVE-2020-0849</a>	CVE-2020-0849   Windows Hard Link Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0848</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0847</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2020-0845</a>	Windows Network Connections Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0844</a>	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0843</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0842</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0841</a>	Windows Hard Link Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0840</a>	Windows Hard Link Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0839</a>	Windows dnssrvr.dll Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0838</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0837</a>	ADFS Spoofing Vulnerability
<a href="#">CVE-2020-0836</a>	Windows DNS Denial of Service Vulnerability
<a href="#">CVE-2020-0834</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2020-0833</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0832</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0831</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0830</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0829</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0828</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2020-0827</a>	Scripting Engine Memory Corruption Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-0826	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0825	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0824	Internet Explorer Memory Corruption Vulnerability
CVE-2020-0823	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0822	Windows Language Pack Installer Elevation of Privilege Vulnerability
CVE-2020-0821	Windows Kernel Information Disclosure Vulnerability
CVE-2020-0820	Media Foundation Information Disclosure Vulnerability
CVE-2020-0819	Windows Device Setup Manager Elevation of Privilege Vulnerability
CVE-2020-0818	Windows Elevation of Privilege Vulnerability
CVE-2020-0817	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0816	Microsoft Edge Memory Corruption Vulnerability
CVE-2020-0814	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0813	Scripting Engine Information Disclosure Vulnerability
CVE-2020-0812	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2020-0811	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2020-0810	Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-0809	Media Foundation Memory Corruption Vulnerability
CVE-2020-0808	Provisioning Runtime Elevation of Privilege Vulnerability
CVE-2020-0807	Media Foundation Memory Corruption Vulnerability
CVE-2020-0806	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0805	Projected Filesystem Security Feature Bypass Vulnerability
CVE-2020-0804	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0803	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0802	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0801	Media Foundation Memory Corruption Vulnerability
CVE-2020-0800	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0799	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0798	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0797	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0796	Windows SMBv3 Client/Server Remote Code Execution Vulnerability
CVE-2020-0794	Windows Denial of Service Vulnerability
CVE-2020-0793	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-0792	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0791	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0790	Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2020-0788	Win32k Elevation of Privilege Vulnerability
CVE-2020-0787	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
CVE-2020-0785	Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2020-0784	DirectX Elevation of Privilege Vulnerability
CVE-2020-0783	Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-0782	Windows Cryptographic Catalog Services Elevation of Privilege Vulnerability
CVE-2020-0781	Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-0780	Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-0779	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0778	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0777	Windows Work Folder Service Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-0776	Windows Elevation of Privilege Vulnerability
CVE-2020-0775	Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-0774	Windows GDI Information Disclosure Vulnerability
CVE-2020-0773	Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0772	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0771	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-0770	Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0769	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-0768	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0767	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0766	Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-0764	Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-0763	Windows Defender Security Center Elevation of Privilege Vulnerability
CVE-2020-0762	Windows Defender Security Center Elevation of Privilege Vulnerability
CVE-2020-0761	Active Directory Remote Code Execution Vulnerability
CVE-2020-0757	Windows SSH Elevation of Privilege Vulnerability
CVE-2020-0756	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0755	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0754	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0753	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0752	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0751	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0750	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0749	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0748	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0747	Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2020-0746	Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2020-0745	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0744	Windows GDI Information Disclosure Vulnerability
CVE-2020-0743	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0742	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0741	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0740	Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0739	Windows Elevation of Privilege Vulnerability
CVE-2020-0738	Media Foundation Memory Corruption Vulnerability
CVE-2020-0737	Windows Elevation of Privilege Vulnerability
CVE-2020-0735	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0734	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0731	Win32k Elevation of Privilege Vulnerability
CVE-2020-0730	Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2020-0729	LNK Remote Code Execution Vulnerability
CVE-2020-0728	Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2020-0727	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0726	Win32k Elevation of Privilege Vulnerability
CVE-2020-0725	Win32k Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-0724	Win32k Elevation of Privilege Vulnerability
CVE-2020-0723	Win32k Elevation of Privilege Vulnerability
CVE-2020-0722	Win32k Elevation of Privilege Vulnerability
CVE-2020-0721	Win32k Elevation of Privilege Vulnerability
CVE-2020-0720	Win32k Elevation of Privilege Vulnerability
CVE-2020-0719	Win32k Elevation of Privilege Vulnerability
CVE-2020-0718	Active Directory Remote Code Execution Vulnerability
CVE-2020-0717	Win32k Information Disclosure Vulnerability
CVE-2020-0716	Win32k Information Disclosure Vulnerability
CVE-2020-0715	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0714	DirectX Information Disclosure Vulnerability
CVE-2020-0713	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0712	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0711	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0710	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0708	Windows Imaging Library Remote Code Execution Vulnerability
CVE-2020-0707	Windows IME Elevation of Privilege Vulnerability
CVE-2020-0706	Microsoft Browser Information Disclosure Vulnerability
CVE-2020-0705	Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability
CVE-2020-0704	Windows Wireless Network Manager Elevation of Privilege Vulnerability
CVE-2020-0703	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-0701	Windows Client License Service Elevation of Privilege Vulnerability
CVE-2020-0699	Win32k Information Disclosure Vulnerability
CVE-2020-0698	Windows Information Disclosure Vulnerability
CVE-2020-0691	Win32k Elevation of Privilege Vulnerability
CVE-2020-0690	DirectX Elevation of Privilege Vulnerability
CVE-2020-0689	Microsoft Secure Boot Security Feature Bypass Vulnerability
CVE-2020-0687	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2020-0686	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0685	Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-0684	LNK Remote Code Execution Vulnerability
CVE-2020-0683	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0682	Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0681	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0680	Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0679	Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0678	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-0677	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0676	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0675	Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0674	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0673	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0672	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0671	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0670	Windows Kernel Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

CVE-2020-0669	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0668	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0667	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0666	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0665	Active Directory Elevation of Privilege Vulnerability
CVE-2020-0664	Active Directory Information Disclosure Vulnerability
CVE-2020-0663	Microsoft Edge Elevation of Privilege Vulnerability
CVE-2020-0662	Internet Connection Sharing Service Remote Code Execution Vulnerability
CVE-2020-0661	Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0660	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2020-0659	Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2020-0658	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0657	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-0655	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2020-0648	Windows RSoP Service Application Elevation of Privilege Vulnerability
CVE-2020-0646	.NET Framework Remote Code Execution Injection Vulnerability
CVE-2020-0645	Microsoft IIS Server Tampering Vulnerability
CVE-2020-0644	Windows Elevation of Privilege Vulnerability
CVE-2020-0643	Windows GDI+ Information Disclosure Vulnerability
CVE-2020-0642	Win32k Elevation of Privilege Vulnerability
CVE-2020-0641	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-0640	Internet Explorer Memory Corruption Vulnerability
CVE-2020-0639	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0638	Update Notification Manager Elevation of Privilege Vulnerability
CVE-2020-0637	Remote Desktop Web Access Information Disclosure Vulnerability
CVE-2020-0636	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2020-0635	Windows Elevation of Privilege Vulnerability
CVE-2020-0634	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-0633	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0632	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0631	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0630	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0629	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0628	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0627	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0626	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0625	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0624	Win32k Elevation of Privilege Vulnerability
CVE-2020-0623	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0620	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2020-0618	Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability
CVE-2020-0616	Microsoft Windows Denial of Service Vulnerability
CVE-2020-0615	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0614	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0613	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0611	Remote Desktop Client Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2020-0610</a>	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability
<a href="#">CVE-2020-0609</a>	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability
<a href="#">CVE-2020-0608</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2020-0607</a>	Microsoft Graphics Components Information Disclosure Vulnerability
<a href="#">CVE-2020-0606</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2020-0605</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2020-0601</a>	Windows CryptoAPI Spoofing Vulnerability

## **2019 – Microsoft® Patches Tested with Pro-Watch**

<a href="#">CVE-2019-1226</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1225</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
<a href="#">CVE-2019-1224</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
.NET	Quality Rollup for .NET Framework
<a href="#">CVE-2019-1488</a>	Microsoft Defender Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1485</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2019-1484</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2019-1483</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1476</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1474</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1472</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1471</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-1470</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2019-1469</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-1468</a>	Win32k Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1467</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1466</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1465</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1458</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1456</a>	OpenType Font Parsing Remote Code Execution Vulnerability
<a href="#">CVE-2019-1453</a>	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
<a href="#">CVE-2019-1439</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1438</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1435</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1434</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1433</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1432</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1429</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1424</a>	NetLogon Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1422</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1419</a>	OpenType Font Parsing Remote Code Execution Vulnerability
<a href="#">CVE-2019-1418</a>	Windows Modules Installer Service Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-1415</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1412</a>	OpenType Font Driver Information Disclosure Vulnerability
<a href="#">CVE-2019-1411</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1409</a>	Windows Remote Procedure Call Information Disclosure Vulnerability
<a href="#">CVE-2019-1408</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1407</a>	Windows Graphics Component Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1406</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1405</a>	Windows UPnP Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1399</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-1397</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-1396</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1395</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1394</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1393</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1392</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1391</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1390</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2019-1389</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-1388</a>	Windows Certificate Dialog Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1384</a>	Microsoft Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1382</a>	Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1381</a>	Microsoft Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-1380</a>	Microsoft splwow64 Elevation of Privilege Vulnerability
<a href="#">CVE-2019-11135</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0860</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-0838</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-0719</a>	Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-0712</a>	Windows Hyper-V Denial of Service Vulnerability
.NET	Quality Rollup for .NET Framework
<a href="#">CVE-2019-1371</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2019-1368</a>	Windows Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1367</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1366</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1365</a>	Microsoft IIS Server Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1359</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1358</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1357</a>	Browser Spoofing Vulnerability
<a href="#">CVE-2019-1356</a>	Microsoft Edge based on Edge HTML Information Disclosure Vulnerability
<a href="#">CVE-2019-1347</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1346</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1345</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1344</a>	Windows Code Integrity Module Information Disclosure Vulnerability
<a href="#">CVE-2019-1343</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1342</a>	Windows Error Reporting Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1341</a>	Windows Power Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1340</a>	Microsoft Windows Elevation of Privilege Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-1339</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1337</a>	Windows Update Client Information Disclosure Vulnerability
<a href="#">CVE-2019-1336</a>	Microsoft Windows Update Client Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1335</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1334</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1333</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-1326</a>	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
<a href="#">CVE-2019-1325</a>	Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1323</a>	Microsoft Windows Update Client Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1322</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1321</a>	Microsoft Windows CloudStore Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1320</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1319</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1318</a>	Microsoft Windows Transport Layer Security Spoofing Vulnerability
<a href="#">CVE-2019-1317</a>	Microsoft Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1315</a>	Windows Error Reporting Manager Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1311</a>	Windows Imaging API Remote Code Execution Vulnerability
<a href="#">CVE-2019-1308</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1307</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1238</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2019-1192</a>	Microsoft Browsers Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1166</a>	Windows NTLM Tampering Vulnerability
<a href="#">CVE-2019-1060</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0608</a>	Microsoft Browser Spoofing Vulnerability
<a href="#">CVE-2019-0537</a>	Microsoft Visual Studio Information Disclosure Vulnerability
.NET	Preview of Quality Rollup for .NET Framework
<a href="#">CVE-2019-1303</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1300</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1299</a>	Microsoft Edge based on Edge HTML Information Disclosure Vulnerability
<a href="#">CVE-2019-1298</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1294</a>	Windows Secure Boot Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1293</a>	Windows SMB Client Driver Information Disclosure Vulnerability
<a href="#">CVE-2019-1292</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1291</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-1290</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-1289</a>	Windows Update Delivery Optimization Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1287</a>	Windows Network Connectivity Assistant Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1286</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1285</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1282</a>	Windows Common Log File System Driver Information Disclosure Vulnerability
<a href="#">CVE-2019-1280</a>	LNK Remote Code Execution Vulnerability
<a href="#">CVE-2019-1278</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1277</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1274</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1273</a>	Active Directory Federation Services XSS Vulnerability
<a href="#">CVE-2019-1272</a>	Windows ALPC Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-1271</a>	Windows Media Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1270</a>	Microsoft Windows Store Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1269</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1268</a>	Winlogon Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1267</a>	Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1256</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1254</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2019-1253</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1252</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1251</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1250</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1249</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1248</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1247</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1246</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1245</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1244</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1243</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1242</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1241</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1240</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1237</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1236</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2019-1235</a>	Windows Text Service Framework Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1232</a>	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1226</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1225</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
<a href="#">CVE-2019-1224</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
<a href="#">CVE-2019-1221</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1220</a>	Microsoft Browser Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1219</a>	Windows Transaction Manager Information Disclosure Vulnerability
<a href="#">CVE-2019-1217</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-1216</a>	DirectX Information Disclosure Vulnerability
<a href="#">CVE-2019-1215</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1214</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1208</a>	VBScript Remote Code Execution Vulnerability
<a href="#">CVE-2019-1142</a>	.NET Framework Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1138</a>	Chakra Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2019-0788</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-0787</a>	Remote Desktop Client Remote Code Execution Vulnerability
<a href="#">CVE-2018-8172</a>	Visual Studio Remote Code Execution Vulnerability
<a href="#">CVE-2018-1037</a>	Microsoft Visual Studio Information Disclosure Vulnerability
.NET	Cumulative Update for Windows 10, Windows 8.1 and Windows Server 2012 R2
<a href="#">CVE-2019-9518</a>	HTTP/2 Server Denial of Service Vulnerability
<a href="#">CVE-2019-9514</a>	HTTP/2 Server Denial of Service Vulnerability
<a href="#">CVE-2019-9513</a>	HTTP/2 Server Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-9512</a>	HTTP/2 Server Denial of Service Vulnerability
<a href="#">CVE-2019-9511</a>	HTTP/2 Server Denial of Service Vulnerability
<a href="#">CVE-2019-9506</a>	Encryption Key Negotiation of Bluetooth Vulnerability
<a href="#">CVE-2019-1227</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1226</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1225</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
<a href="#">CVE-2019-1224</a>	Remote Desktop Protocol Server Information Disclosure Vulnerability
<a href="#">CVE-2019-1223</a>	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
<a href="#">CVE-2019-1222</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1212</a>	Windows DHCP Server Denial of Service Vulnerability
<a href="#">CVE-2019-1206</a>	Windows DHCP Server Denial of Service Vulnerability
<a href="#">CVE-2019-1198</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1190</a>	Windows Image Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1188</a>	LNK Remote Code Execution Vulnerability
<a href="#">CVE-2019-1187</a>	XmlLite Runtime Denial of Service Vulnerability
<a href="#">CVE-2019-1186</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1184</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1183</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1182</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1181</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-1180</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1179</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1178</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1177</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1176</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1175</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1174</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1173</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1172</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-1171</a>	SymCrypt Information Disclosure Vulnerability
<a href="#">CVE-2019-1170</a>	Windows NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1168</a>	Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1164</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1163</a>	Windows File Signature Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1162</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1159</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1158</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2019-1157</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1156</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1155</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1153</a>	Microsoft Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2019-1152</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1151</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1150</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1149</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1148</a>	Microsoft Graphics Component Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-1147</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1146</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-1145</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1144</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2019-1143</a>	Windows Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2019-1078</a>	Microsoft Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2019-1057</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0965</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-0736</a>	Windows DHCP Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-0723</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0720</a>	Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-0718</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0717</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0716</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-0715</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0714</a>	Windows Hyper-V Denial of Service Vulnerability
.NET	Cumulative Update for Windows 10, Windows Server 2012 R2 and Windows Server 2016
<a href="#">CVE-2019-1130</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1129</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1128</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1127</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1126</a>	ADFS Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1124</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1123</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1122</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1121</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1120</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1119</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1118</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1117</a>	DirectWrite Remote Code Execution Vulnerability
<a href="#">CVE-2019-1113</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2019-1108</a>	Remote Desktop Protocol Client Information Disclosure Vulnerability
<a href="#">CVE-2019-1102</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2019-1097</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1096</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-1095</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1094</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1093</a>	DirectWrite Information Disclosure Vulnerability
<a href="#">CVE-2019-1091</a>	Microsoft unistore.dll Information Disclosure Vulnerability
<a href="#">CVE-2019-1090</a>	Windows RPCSS Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1089</a>	Windows RPCSS Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1088</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1087</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1086</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1085</a>	Windows WLAN Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1083</a>	.NET Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-1082</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1074</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1073</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1071</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1067</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1037</a>	Windows Error Reporting Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1006</a>	WCF/WIF SAML Token Authentication Bypass Vulnerability
<a href="#">CVE-2019-0975</a>	ADFS Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0966</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0887</a>	Remote Desktop Services Remote Code Execution Vulnerability
<a href="#">CVE-2019-0880</a>	Microsoft splwow64 Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0865</a>	SymCrypt Denial of Service Vulnerability
<a href="#">CVE-2019-0811</a>	Windows DNS Server Denial of Service Vulnerability
<a href="#">CVE-2019-0785</a>	Windows DHCP Server Remote Code Execution Vulnerability
<a href="#">CVE-2019-0683</a>	Active Directory Elevation of Privilege Vulnerability
.NET	Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10, version 1809
<a href="#">CVE-2019-1069</a>	Task Scheduler Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1065</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1064</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1053</a>	Windows Shell Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1050</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1046</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1045</a>	Windows Network File System Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1044</a>	Windows Secure Kernel Mode Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1043</a>	Comctl32 Remote Code Execution Vulnerability
<a href="#">CVE-2019-1041</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1040</a>	Windows NTLM Tampering Vulnerability
<a href="#">CVE-2019-1039</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-1028</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1027</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1026</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1025</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-1022</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1021</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1019</a>	Microsoft Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-1018</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1017</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1014</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-1012</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1010</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-1007</a>	Windows Audio Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0998</a>	Windows Storage Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0986</a>	Windows User Profile Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0984</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0983</a>	Windows Storage Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0974</a>	Jet Database Engine Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-0973</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0972</a>	Local Security Authority Subsystem Service Denial of Service Vulnerability
<a href="#">CVE-2019-0959</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0948</a>	Windows Event Viewer Information Disclosure Vulnerability
<a href="#">CVE-2019-0943</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0941</a>	Microsoft IIS Server Denial of Service Vulnerability
<a href="#">CVE-2019-0909</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0908</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0907</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0906</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0905</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0904</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0888</a>	ActiveX Data Objects (ADO) Remote Code Execution Vulnerability
<a href="#">CVE-2019-0722</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-0713</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0711</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0710</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0620</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2019-0981</a>	.Net Framework and .Net Core Denial of Service Vulnerability
<a href="#">CVE-2019-0980</a>	.Net Framework and .Net Core Denial of Service Vulnerability
<a href="#">CVE-2019-0683</a>	Active Directory Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0961</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0942</a>	Unified Write Filter Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0936</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0931</a>	Windows Storage Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0903</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2019-0902</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0901</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0900</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0899</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0898</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0897</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0896</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0895</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0894</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0893</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0892</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0891</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0890</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0889</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0886</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2019-0885</a>	Windows OLE Remote Code Execution Vulnerability
<a href="#">CVE-2019-0882</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0881</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0864</a>	.NET Framework Denial of Service Vulnerability
<a href="#">CVE-2019-0863</a>	Windows Error Reporting Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-0820</a>	.NET Framework and .NET Core Denial of Service Vulnerability
<a href="#">CVE-2019-0758</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0734</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0733</a>	Windows Defender Application Control Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0727</a>	Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0725</a>	Windows DHCP Server Remote Code Execution Vulnerability
<a href="#">CVE-2019-0707</a>	Windows NDIS Elevation of Privilege Vulnerability
.NET	No .NET Framework updates for April 2019
<a href="#">CVE-2019-0674</a>	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0673</a>	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0671</a>	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0879</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0877</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0859</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0856</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2019-0853</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2019-0851</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0849</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0848</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-0847</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0846</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0845</a>	Windows IOleCvt Interface Remote Code Execution Vulnerability
<a href="#">CVE-2019-0844</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0842</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0841</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0840</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0839</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-0838</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-0836</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0814</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-0805</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0803</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0802</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0796</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0795</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0794</a>	OLE Automation Remote Code Execution Vulnerability
<a href="#">CVE-2019-0793</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0792</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0791</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0790</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0786</a>	Hyper-V vSMB Remote Code Execution Vulnerability
<a href="#">CVE-2019-0735</a>	Windows CSRSS Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0732</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0731</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0730</a>	Windows Elevation of Privilege Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-0688</a>	Windows TCP/IP Information Disclosure Vulnerability
<a href="#">CVE-2019-0685</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">.NET</a>	No .NET Framework updates for March 2019
<a href="#">CVE-2019-0601</a>	HID Information Disclosure Vulnerability
<a href="#">CVE-2019-0821</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2019-0797</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0784</a>	Windows ActiveX Remote Code Execution Vulnerability
<a href="#">CVE-2019-0782</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0776</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-0775</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0774</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0772</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0767</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0766</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0765</a>	Comctl32 Remote Code Execution Vulnerability
<a href="#">CVE-2019-0759</a>	Windows Print Spooler Information Disclosure Vulnerability
<a href="#">CVE-2019-0756</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2019-0755</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0754</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2019-0726</a>	Windows DHCP Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-0704</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2019-0703</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2019-0702</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0701</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0698</a>	Windows DHCP Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-0697</a>	Windows DHCP Client Remote Code Execution Vulnerability
<a href="#">CVE-2019-0696</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0695</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0694</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0693</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0692</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0690</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2019-0689</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0682</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0617</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0614</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0603</a>	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
<a href="#">CVE-2019-0664</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0663</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0662</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2019-0660</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0659</a>	Windows Storage Service Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0656</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0637</a>	Windows Defender Firewall Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0636</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2019-0635</a>	Windows Hyper-V Information Disclosure Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2019-0633</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2019-0632</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0631</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0630</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2019-0628</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2019-0627</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2019-0626</a>	Windows DHCP Server Remote Code Execution Vulnerability
<a href="#">CVE-2019-0625</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0623</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0621</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0619</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0618</a>	GDI+ Remote Code Execution Vulnerability
<a href="#">CVE-2019-0616</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0615</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0602</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2019-0601</a>	HID Information Disclosure Vulnerability
<a href="#">CVE-2019-0600</a>	HID Information Disclosure Vulnerability
<a href="#">CVE-2019-0599</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0598</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0597</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0596</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0595</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0555</a>	Microsoft XmlDocument Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0584</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0583</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0582</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0581</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0580</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0579</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0578</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0577</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0576</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0575</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0570</a>	Windows Runtime Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0569</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0555</a>	Microsoft XmlDocument Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0554</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0552</a>	Windows COM Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0549</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2019-0543</a>	Microsoft Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2019-0538</a>	Jet Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2019-0536</a>	Windows Kernel Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-0859</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-12207</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2018-8641</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8639</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8637</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2018-8634</a>	Microsoft Text-To-Speech Remote Code Execution Vulnerability
<a href="#">CVE-2018-8626</a>	Windows DNS Server Heap Overflow Vulnerability
<a href="#">CVE-2018-8622</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8612</a>	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
<a href="#">CVE-2018-8611</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8599</a>	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8596</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8595</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8514</a>	Remote Procedure Call runtime Information Disclosure Vulnerability
<a href="#">CVE-2018-8477</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8584</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8565</a>	Win32k Information Disclosure Vulnerability
<a href="#">CVE-2018-8563</a>	DirectX Information Disclosure Vulnerability
<a href="#">CVE-2018-8562</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8561</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8554</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8553</a>	Microsoft Graphics Components Remote Code Execution Vulnerability
<a href="#">CVE-2018-8552</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-8550</a>	Windows COM Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8549</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8547</a>	Active Directory Federation Services XSS Vulnerability
<a href="#">CVE-2018-8544</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8485</a>	DirectX Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8476</a>	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
<a href="#">CVE-2018-8471</a>	Microsoft RemoteFX Virtual GPU miniport driver Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8454</a>	Windows Audio Service Information Disclosure Vulnerability
<a href="#">CVE-2018-8450</a>	Windows Search Remote Code Execution Vulnerability
<a href="#">CVE-2018-8417</a>	Microsoft JScript Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8415</a>	Microsoft PowerShell Tampering Vulnerability
<a href="#">CVE-2018-8408</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8407</a>	Remote Procedure Call runtime Information Disclosure Vulnerability
<a href="#">CVE-2018-8256</a>	Microsoft PowerShell Remote Code Execution Vulnerability
<a href="#">CVE-2018-8506</a>	Microsoft Windows Codecs Library Information Disclosure Vulnerability
<a href="#">CVE-2018-8497</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8495</a>	Windows Shell Remote Code Execution Vulnerability
<a href="#">CVE-2018-8494</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2018-8493</a>	Windows TCP/IP Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-8492</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8489</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2018-8486</a>	DirectX Information Disclosure Vulnerability
<a href="#">CVE-2018-8484</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8482</a>	Windows Media Player Information Disclosure Vulnerability
<a href="#">CVE-2018-8481</a>	Windows Media Player Information Disclosure Vulnerability
<a href="#">CVE-2018-8472</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8453</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8423</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8413</a>	Windows Theme API Remote Code Execution Vulnerability
<a href="#">CVE-2018-8411</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8333</a>	Microsoft Filter Manager Elevation Of Privilege Vulnerability
<a href="#">CVE-2018-8330</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8329</a>	Linux On Windows Elevation Of Privilege Vulnerability
<a href="#">CVE-2018-8320</a>	Windows DNS Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8475</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2018-8468</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8455</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8446</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8444</a>	Windows SMB Information Disclosure Vulnerability
<a href="#">CVE-2018-8443</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8442</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8440</a>	Windows ALPC Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8439</a>	Windows Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2018-8438</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2018-8434</a>	Windows Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2018-8433</a>	Microsoft Graphics Component Information Disclosure Vulnerability
<a href="#">CVE-2018-8424</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8420</a>	MS XML Remote Code Execution Vulnerability
<a href="#">CVE-2018-8419</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8410</a>	Windows Registry Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8393</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8392</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8335</a>	Windows SMB Denial of Service Vulnerability
<a href="#">CVE-2018-8332</a>	Win32k Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-8271</a>	Windows Information Disclosure Vulnerability
<a href="#">CVE-2018-8414</a>	Windows Shell Remote Code Execution Vulnerability
<a href="#">CVE-2018-8406</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8405</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8404</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8401</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8400</a>	DirectX Graphics Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8399</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8398</a>	Windows GDI Information Disclosure Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-8394</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8360</a>	.NET Framework Information Disclosure Vulnerability
<a href="#">CVE-2018-8350</a>	Windows PDF Remote Code Execution Vulnerability
<a href="#">CVE-2018-8349</a>	Microsoft COM for Windows Remote Code Execution Vulnerability
<a href="#">CVE-2018-8348</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8347</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8345</a>	LNK Remote Code Execution Vulnerability
<a href="#">CVE-2018-8344</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-8343</a>	Windows NDIS Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8341</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8340</a>	AD FS Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8339</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8204</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8202</a>	.NET Framework Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8200</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-0952</a>	Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8356</a>	.NET Framework Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8314</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8313</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8309</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2018-8308</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8307</a>	WordPad Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8304</a>	Windows DNSAPI Denial of Service Vulnerability
<a href="#">CVE-2018-8284</a>	.NET Framework Remote Code Injection Vulnerability
<a href="#">CVE-2018-8282</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8260</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2018-8242</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-8222</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8206</a>	Windows FTP Server Denial of Service Vulnerability
<a href="#">CVE-2018-8202</a>	.NET Framework Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8251</a>	Media Foundation Memory Corruption Vulnerability
<a href="#">CVE-2018-8239</a>	Windows GDI Information Disclosure Vulnerability
<a href="#">CVE-2018-8233</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8231</a>	HTTP Protocol Stack Remote Code Execution Vulnerability
<a href="#">CVE-2018-8226</a>	HTTP.sys Denial of Service Vulnerability
<a href="#">CVE-2018-8225</a>	Windows DNSAPI Remote Code Execution Vulnerability
<a href="#">CVE-2018-8221</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8219</a>	Hypervisor Code Integrity Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8215</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8214</a>	Windows Desktop Bridge Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8213</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2018-8212</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8211</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8210</a>	Windows Remote Code Execution Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-8208</a>	Windows Desktop Bridge Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8207</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8205</a>	Windows Denial of Service Vulnerability
<a href="#">CVE-2018-8201</a>	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
<a href="#">CVE-2018-8175</a>	WEBDAV Denial of Service Vulnerability
<a href="#">CVE-2018-8169</a>	HIDParser Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8140</a>	Cortana Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8121</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0982</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2018-1040</a>	Windows Code Integrity Module Denial of Service Vulnerability
<a href="#">CVE-2018-1036</a>	NTFS Elevation of Privilege Vulnerability
<a href="#">CVE-2018-1003</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8897</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8174</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-8167</a>	Windows Common Log File System Driver Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8166</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8164</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8136</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2018-8134</a>	Windows Elevation of Privilege Vulnerability
<a href="#">CVE-2018-8127</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-8124</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0959</a>	Hyper-V Remote Code Execution Vulnerability
<a href="#">CVE-2018-0824</a>	Microsoft COM for Windows Remote Code Execution Vulnerability
<a href="#">CVE-2018-8116</a>	Microsoft Graphics Component Denial of Service Vulnerability
<a href="#">CVE-2018-1035</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2018-1016</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-1015</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-1013</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-1012</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-1010</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2018-1009</a>	Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability
<a href="#">CVE-2018-1008</a>	Graphics Component Font Parsing Elevation of Privilege Vulnerability
<a href="#">CVE-2018-1004</a>	Windows VBScript Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-1003</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2018-0976</a>	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
<a href="#">CVE-2018-0975</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0974</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0973</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0972</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0971</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0970</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0969</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0968</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0967</a>	Windows SNMP Service Denial of Service Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-0966</a>	Device Guard Security Feature Bypass Vulnerability
<a href="#">CVE-2018-0964</a>	Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2018-0963</a>	Windows Kernel Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0960</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0957</a>	Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2018-0956</a>	HTTP.sys Denial of Service Vulnerability
<a href="#">CVE-2018-0890</a>	Active Directory Security Feature Bypass Vulnerability
<a href="#">CVE-2018-0887</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0983</a>	Windows Storage Services Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0977</a>	Win32k Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0926</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0904</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0901</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0900</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0899</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0898</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0897</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0896</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0895</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0894</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0888</a>	Hyper-V Information Disclosure Vulnerability
<a href="#">CVE-2018-0886</a>	CredSSP Remote Code Execution Vulnerability
<a href="#">CVE-2018-0885</a>	Windows Hyper-V Denial of Service Vulnerability
<a href="#">CVE-2018-0884</a>	Windows Security Feature Bypass Vulnerability
<a href="#">CVE-2018-0883</a>	Windows Shell Remote Code Execution Vulnerability
<a href="#">CVE-2018-0881</a>	Microsoft Video Control Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0880</a>	Windows Desktop Bridge Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0878</a>	Windows Remote Assistance Information Disclosure Vulnerability
<a href="#">CVE-2018-0868</a>	Windows Installer Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0817</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0816</a>	Windows GDI Elevation of Privilege Vulnerability
<a href="#">CVE-2018-0814</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0813</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0811</a>	Windows Kernel Information Disclosure Vulnerability
<a href="#">CVE-2018-0800</a>	Scripting Engine Information Disclosure Vulnerability
<a href="#">CVE-2018-0781</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0780</a>	Scripting Engine Information Disclosure Vulnerability
<a href="#">CVE-2018-0778</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0777</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0776</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0800</a>	Scripting Engine Information Disclosure Vulnerability
<a href="#">CVE-2018-0781</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0780</a>	Scripting Engine Information Disclosure Vulnerability
<a href="#">CVE-2018-0778</a>	Scripting Engine Memory Corruption Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2018-0777</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0776</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0775</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0774</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0773</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0772</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0770</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0769</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0767</a>	Scripting Engine Information Disclosure Vulnerability
<a href="#">CVE-2018-0762</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2018-0758</a>	Scripting Engine Memory Corruption Vulnerability

## **2017 – Microsoft® Patches Tested with Pro-Watch**

---

<a href="#">CVE-2017-11918</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11914</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11912</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11911</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11910</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11909</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11908</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11907</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11905</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11903</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11901</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11895</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11894</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11893</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11890</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11889</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11888</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-11886</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11873</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11871</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11870</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11869</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11866</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11862</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11861</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11858</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11856</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-11855</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-11846</a>	Scripting Engine Memory Corruption Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2017-11845</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11843</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11841</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11840</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11839</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11838</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11837</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11836</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11822</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-11821</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11819</a>	Windows Shell Remote Code Execution Vulnerability
<a href="#">CVE-2017-11813</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-11812</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11811</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11810</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11809</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11808</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11807</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11806</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11805</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11804</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11802</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11801</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11800</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11799</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11798</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11797</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11796</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11793</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11792</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11779</a>	Windows DNSAPI Remote Code Execution Vulnerability
<a href="#">CVE-2017-11771</a>	Windows Search Remote Code Execution Vulnerability
<a href="#">CVE-2017-11766</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-11764</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-11763</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2017-11762</a>	Microsoft Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2017-8759</a>	.NET Framework Remote Code Execution Vulnerability
<a href="#">CVE-2017-8750</a>	Microsoft Browser Memory Corruption Vulnerability
<a href="#">CVE-2017-8749</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-8748</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8747</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8741</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8740</a>	Scripting Engine Memory Corruption Vulnerability



<http://buildings.honeywell.com/security>

<a href="#">CVE-2017-8737</a>	Microsoft PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-8734</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8728</a>	Microsoft PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-8727</a>	Windows Shell Memory Corruption Vulnerability
<a href="#">CVE-2017-8727</a>	Microsoft PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-8682</a>	Win32k Graphics Remote Code Execution Vulnerability
<a href="#">CVE-2017-8674</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8672</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8671</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8670</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8669</a>	Microsoft Browser Memory Corruption Vulnerability
<a href="#">CVE-2017-8661</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8660</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8657</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8656</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8655</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8653</a>	Microsoft Browser Memory Corruption Vulnerability
<a href="#">CVE-2017-8649</a>	Microsoft Browser Memory Corruption Vulnerability
<a href="#">CVE-2017-8647</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8646</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8645</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8641</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8640</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8639</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8638</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8636</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8635</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8634</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8622</a>	Windows Subsystem for Linux Elevation of Privilege Vulnerability
<a href="#">CVE-2017-8620</a>	Windows Search Remote Code Execution Vulnerability
<a href="#">CVE-2017-8619</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8618</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8617</a>	Microsoft Edge Remote Code Execution Vulnerability
<a href="#">CVE-2017-8610</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8609</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8608</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8607</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8606</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8604</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8603</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8601</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8598</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8596</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8594</a>	Internet Explorer Memory Corruption Vulnerability

Honeywell Commercial Security  
715 Peachtree St.NE  
Atlanta, GA 30308

<http://buildings.honeywell.com/security>

- [CVE-2017-8591](#) Windows IME Remote Code Execution Vulnerability
- [CVE-2017-8589](#) Windows Search Remote Code Execution Vulnerability
- [CVE-2017-8549](#) Scripting Engine Memory Corruption Vulnerability
- [CVE-2017-8548](#) Scripting Engine Memory Corruption Vulnerability
- [CVE-2017-8543](#) Windows Search Remote Code Execution Vulnerability
- [CVE-2017-8528](#) Windows Uniscribe Remote Code Execution Vulnerability
- [CVE-2017-8527](#) Windows Graphics Remote Code Execution Vulnerability
- [CVE-2017-8524](#) Scripting Engine Memory Corruption Vulnerability
- [CVE-2017-8522](#) Scripting Engine Memory Corruption Vulnerability
- [CVE-2017-8520](#) Scripting Engine Memory Corruption Vulnerability

<http://buildings.honeywell.com/security>

<a href="#">CVE-2017-8517</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8499</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-8497</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8496</a>	Microsoft Edge Memory Corruption Vulnerability
<a href="#">CVE-2017-8464</a>	LNK Remote Code Execution Vulnerability
<a href="#">CVE-2017-8463</a>	Windows Explorer Remote Code Execution Vulnerability
<a href="#">CVE-2017-0293</a>	Windows PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-0292</a>	Windows PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-0291</a>	Windows PDF Remote Code Execution Vulnerability
<a href="#">CVE-2017-0283</a>	Windows Uniscribe Remote Code Execution Vulnerability
<a href="#">CVE-2017-0279</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2017-0278</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2017-0277</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2017-0272</a>	Windows SMB Remote Code Execution Vulnerability
<a href="#">CVE-2017-0250</a>	Microsoft JET Database Engine Remote Code Execution Vulnerability
<a href="#">CVE-2017-0228</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-0202</a>	Internet Explorer Memory Corruption Vulnerability
<a href="#">CVE-2017-0201</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">CVE-2017-0181</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2017-0180</a>	Windows Remote Code Execution Vulnerability
<a href="#">CVE-2017-0161</a>	NetBIOS Remote Code Execution Vulnerability
<a href="#">CVE-2017-0160</a>	.NET Remote Code Execution Vulnerability
<a href="#">CVE-2017-0158</a>	Scripting Engine Memory Corruption Vulnerability
<a href="#">MS17-023</a>	Security Update for Adobe Flash Player (4014329)
<a href="#">MS17-022</a>	Security Update for Microsoft XML Core Services (4010321)
<a href="#">MS17-018</a>	Security Update for Windows Kernel-Mode Drivers (4013083)
<a href="#">MS17-017</a>	Security Update for Windows Kernel (4013081)
<a href="#">MS17-016</a>	Security Update for Windows IIS (4013074)
<a href="#">MS17-013</a>	Security Update for Microsoft Graphics Component (4013075)
<a href="#">MS17-012</a>	Security Update for Microsoft Windows (4013078)
<a href="#">MS17-011</a>	Security Update for Microsoft Uniscribe (4013076)
<a href="#">MS17-010</a>	Security Update for Microsoft Windows SMB Server (4013389)
<a href="#">MS17-009</a>	Security Update for Microsoft Windows PDF Library (4010319)
<a href="#">MS17-008</a>	Security Update for Windows Hyper-V (4013082)
<a href="#">MS17-007</a>	Cumulative Security Update for Microsoft Edge (4013071)
<a href="#">MS17-006</a>	Cumulative Security Update for Internet Explorer (4013073)
<a href="#">MS17-003</a>	Security Update for Adobe Flash Player (3214628)
<a href="#">MS17-001</a>	Security Update for Microsoft Edge (3214288)

<http://buildings.honeywell.com/security>

## **2016 – Microsoft® Patches Tested with Pro-Watch**

---

<a href="#">MS16-155</a>	Security Update for .NET Framework (3205640)
<a href="#">MS16-154</a>	Security Update for Adobe Flash Player (3209498)
<a href="#">MS16-153</a>	Security Update for Common Log File System Driver (3207328)
<a href="#">MS16-152</a>	Security Update for Windows Kernel (3199709)
<a href="#">MS16-151</a>	Security Update for Windows Kernel-Mode Drivers (3205651)
<a href="#">MS16-150</a>	Security Update for Secure Kernel Mode (3205642)
<a href="#">MS16-149</a>	Security Update for Microsoft Windows (3205655)
<a href="#">MS16-147</a>	Security Update for Microsoft Uniscribe (3204063)
<a href="#">MS16-146</a>	Security Update for Microsoft Graphics Component (3204066)
<a href="#">MS16-145</a>	Cumulative Security Update for Microsoft Edge (3204062)
<a href="#">MS16-144</a>	Cumulative Security Update for Internet Explorer (3204059)
<a href="#">MS16-142</a>	Cumulative Security Update for Internet Explorer (3198467)
<a href="#">MS16-141</a>	Security Update for Adobe Flash Player (3202790)
<a href="#">MS16-140</a>	Security Update for Boot Manager (3193479)
<a href="#">MS16-138</a>	Security Update for Microsoft Virtual Hard Disk Driver (3199647)
<a href="#">MS16-137</a>	Security Update for Windows Authentication Methods (3199173)
<a href="#">MS16-136</a>	Security Update for SQL Server (3199641)
<a href="#">MS16-135</a>	Security Update for Windows Kernel-Mode Drivers (3199135)
<a href="#">MS16-134</a>	Security Update for Common Log File System Driver (3193706)
<a href="#">MS16-132</a>	Security Update for Microsoft Graphics Component (3199120)
<a href="#">MS16-131</a>	Security Update for Microsoft Video Control (3199151)
<a href="#">MS16-130</a>	Security Update for Microsoft Windows (3199172)
<a href="#">MS16-129</a>	Cumulative Security Update for Microsoft Edge (3199057)
<a href="#">MS16-128</a>	Security Update for Adobe Flash Player (3201860)
<a href="#">MS16-127</a>	Security Update for Adobe Flash Player (3194343)
<a href="#">MS16-125</a>	Security Update for Diagnostics Hub (3193229)
<a href="#">MS16-124</a>	Security Update for Windows Registry (3193227)
<a href="#">MS16-123</a>	Security Update for Windows Kernel-Mode Drivers (3192892)
<a href="#">MS16-122</a>	Security Update for Microsoft Video Control (3195360)
<a href="#">MS16-120</a>	Security Update for Microsoft Graphics Component (3192884)
<a href="#">MS16-119</a>	Cumulative Security Update for Microsoft Edge (3192890)
<a href="#">MS16-118</a>	Cumulative Security Update for Internet Explorer (3192887)
<a href="#">MS16-117</a>	Security Update for Adobe Flash Player (3188128)
<a href="#">MS16-116</a>	Security Update in OLE Automation for VBScript Scripting Engine (3188724)
<a href="#">MS16-115</a>	Security Update for Microsoft Windows PDF Library (3188733)

<http://buildings.honeywell.com/security>

<a href="#">MS16-114</a>	Security Update for SMBv1 Server (3185879)
<a href="#">MS16-112</a>	Security Update for Windows Lock Screen (3178469)
<a href="#">MS16-111</a>	Security Update for Windows Kernel (3186973)
<a href="#">MS16-106</a>	Security Update for Microsoft Graphics Component (3185848)
<a href="#">MS16-105</a>	Cumulative Security Update for Microsoft Edge (3183043)
<a href="#">MS16-104</a>	Cumulative Security Update for Internet Explorer (3183038)
<a href="#">MS16-103</a>	Security Update for ActiveSyncProvider (3182332)
<a href="#">MS16-102</a>	Security Update for Microsoft Windows PDF Library (3182248)
<a href="#">MS16-101</a>	Security Update for Windows Authentication Methods (3178465)
<a href="#">MS16-100</a>	Security Update for Secure Boot (3177404)
<a href="#">MS16-098</a>	Security Update for Windows Kernel-Mode Drivers (3178466)
<a href="#">MS16-097</a>	Security Update for Microsoft Graphics Component (3177393)
<a href="#">MS16-096</a>	Cumulative Security Update for Microsoft Edge (3177358)
<a href="#">MS16-095</a>	Cumulative Security Update for Internet Explorer (3177356)
<a href="#">MS16-094</a>	Security Update for Secure Boot (3177404)
<a href="#">MS16-093</a>	Security Update for Adobe Flash Player (3174060)
<a href="#">MS16-092</a>	Security Update for Windows Kernel (3171910)
<a href="#">MS16-091</a>	Security Update for .NET Framework (3170048)
<a href="#">MS16-090</a>	Security Update for Windows Kernel-Mode Drivers (3171481)
<a href="#">MS16-089</a>	Security Update for Windows Secure Kernel Mode (3170050)
<a href="#">MS16-087</a>	Security Update for Windows Print Spooler Components (3170005)
<a href="#">MS16-085</a>	Cumulative Security Update for Microsoft Edge (3169999)
<a href="#">MS16-084</a>	Cumulative Security Update for Internet Explorer (3169991)
<a href="#">MS16-082</a>	Security Update for Microsoft Windows Search Component (3165270)
<a href="#">MS16-080</a>	Security Update for Microsoft Windows PDF (3164302)
<a href="#">MS16-077</a>	Security Update for WPAD (3165191)
<a href="#">MS16-076</a>	Security Update for Netlogon (3167691)
<a href="#">MS16-075</a>	Security Update for Windows SMB Server (3164038)
<a href="#">MS16-074</a>	Security Update for Microsoft Graphics Component (3164036)
<a href="#">MS16-073</a>	Security Update for Windows Kernel-Mode Drivers (3164028)
<a href="#">MS16-072</a>	Security Update for Group Policy (3163622)
<a href="#">MS16-067</a>	Security Update for Volume Manager Driver (3155784)
<a href="#">MS16-063</a>	Cumulative Security Update for Internet Explorer (3163649)
<a href="#">MS16-065</a>	Security Update for .NET Framework (3156757)
<a href="#">MS16-064</a>	Security Update for Adobe Flash Player (3157993)
<a href="#">MS16-062</a>	Security Update for Windows Kernel-Mode Drivers (3158222)
<a href="#">MS16-061</a>	Security Update for Microsoft RPC (3155520)
<a href="#">MS16-060</a>	Security Update for Windows Kernel (3154846)

<http://buildings.honeywell.com/security>

- [MS16-057](#) Security Update for Windows Shell (3156987)
- [MS16-056](#) Security Update for Windows Journal (3156761)
- [MS16-055](#) Security Update for Microsoft Graphics Component (3156754)
- [MS16-051](#) Cumulative Security Update for Internet Explorer (3155533)
- [MS16-050](#) Security Update for Adobe Flash Player (3154132)
- [MS16-048](#) Security Update for CSRSS (3148528)
- [MS16-047](#) Security Update for SAM and LSAD Remote Protocols (3148527)
- [MS16-045](#) Security Update for Windows Hyper-V (3143118)
- [MS16-044](#) Security Update for Windows OLE (3146706)
- [MS16-040](#) Security Update for Microsoft XML Core Services (3148541)
- [MS16-039](#) Security Update for Microsoft Graphics Component (3148522)
- [MS16-037](#) Cumulative Security Update for Internet Explorer (3148531)
- [MS16-035](#) Security Update for .NET Framework to Address Security Feature Bypass (3141780)
- [MS16-034](#) Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)
- [MS16-033](#) Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)
- [MS16-032](#) Security Update for Secondary Logon to Address Elevation of Privilege (3143141)
- [MS16-030](#) Security Update for Windows OLE to Address Remote Code Execution (3143136)
- [MS16-028](#) Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)
- [MS16-027](#) Security Update for Windows Media to Address Remote Code Execution (3143146)
- [MS16-026](#) Security Update for Graphic Fonts to Address Remote Code Execution (3143148)
- [MS16-023](#) Cumulative Security Update for Internet Explorer (3142015)
- [MS16-022](#) Security Update for Adobe Flash Player (3135782)
- [MS16-021](#) Security Update for NPS RADIUS Server to Address Denial of Service (3133043)
- [MS16-020](#) Security Update for Active Directory Federation Services to Address Denial of Service (3134222)
- [MS16-019](#) Security Update for .NET Framework to Address Denial of Service (3137893)
- [MS16-018](#) Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)
- [MS16-017](#) Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)
- [MS16-016](#) Security Update for WebDAV to Address Elevation of Privilege (3136041)
- [MS16-014](#) Security Update for Microsoft Windows to Address Remote Code Execution (3134228)
- [MS16-013](#) Security Update for Windows Journal to Address Remote Code Execution (3134811)
- [MS16-012](#) Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)
- [MS16-009](#) Cumulative Security Update for Internet Explorer (3134220)
- [MS16-008](#) Security Update for Windows Kernel to Address Elevation of Privilege (3124605)
- [MS16-007](#) Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
- [MS16-006](#) Security Update for Silverlight to Address Remote Code Execution (3126036)
- [MS16-005](#) Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)
- [MS16-001](#) Cumulative Security Update for Internet Explorer (3124903)

<http://buildings.honeywell.com/security>

## **2015 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS15-135](#) Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)
- [MS15-133](#) Security Update for Windows PGM to Address Elevation of Privilege (3116130)
- [MS15-132](#) Security Update for Microsoft Windows to Address Remote Code Execution (3116162)
- [MS15-130](#) Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)
- [MS15-128](#) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)
- [MS15-124](#) Cumulative Security Update for Internet Explorer (3116180)
- [MS15-122](#) Security Update for Kerberos to Address Security Feature Bypass (3105256)
- [MS15-121](#) Security Update for Schannel to Address Spoofing (3081320)
- [MS15-120](#) Security Update for IPSec to Address Denial of Service (3102939)
- [MS15-119](#) Security Update for Winsock to Address Elevation of Privilege (3104521)
- [MS15-118](#) Security Update for .NET Framework to Address Elevation of Privilege (3104507)
- [MS15-117](#) Security Update for NDIS to Address Elevation of Privilege (3101722)
- [MS15-115](#) Security Update for Microsoft Windows to Address Remote Code Execution (3105864)
- [MS15-114](#) Security Update for Windows Journal to Address Remote Code Execution (3100213)
- [MS15-112](#) Cumulative Security Update for Internet Explorer (3104517)
- [MS15-111](#) Security Update for Windows Kernel to Address Elevation of Privilege (3096447)
- [MS15-109](#) Security Update for Windows Shell to Address Remote Code Execution (3096443)
- [MS15-106](#) Cumulative Security Update for Internet Explorer (3096441)
- [MS15-105](#) Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)
- [MS15-102](#) Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)
- [MS15-101](#) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)
- [MS15-098](#) Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)
- [MS15-097](#) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)
- [MS15-096](#) Vulnerability in Active Directory Service Could Allow Denial of Service (3072595)
- [MS15-094](#) Cumulative Security Update for Internet Explorer (3089548)
- [MS15-092](#) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)
- [MS15-090](#) Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3060716)
- [MS15-089](#) Vulnerability in WebDAV Could Allow Information Disclosure (3076949)
- [MS15-088](#) Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)
- [MS15-085](#) Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)
- [MS15-084](#) Vulnerabilities in XML Core Services Could Allow Information Disclosure (3080129)
- [MS15-082](#) Vulnerabilities in RDP Could Allow Remote Code Execution (3080348)
- [MS15-080](#) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)
- [MS15-079](#) Cumulative Security Update for Internet Explorer (3082442)
- [MS15-077](#) Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)
- [MS15-076](#) Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)

<http://buildings.honeywell.com/security>

- [MS15-075](#) Vulnerabilities in OLE Could Allow Elevation of Privilege (3072633)
- [MS15-074](#) Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (3072630)
- [MS15-073](#) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)
- [MS15-072](#) Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)
- [MS15-071](#) Vulnerability in Netlogon Could Allow Elevation of Privilege (3068457)
- [MS15-069](#) Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)
- [MS15-068](#) Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution (3072000)
- [MS15-067](#) Vulnerability in RDP Could Allow Remote Code Execution (3073094)
- [MS15-065](#) Security Update for Internet Explorer (3076321)
- [MS15-061](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)
- [MS15-060](#) Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (3059317)
- [MS15-058](#) Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718)
- [MS15-057](#) Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)
- [MS15-056](#) Cumulative Security Update for Internet Explorer (3058515)
- [MS15-055](#) Vulnerability in Schannel Could Allow Information Disclosure (3061518)
- [MS15-054](#) Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service (3051768)
- [MS15-052](#) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)
- [MS15-051](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)
- [MS15-050](#) Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)
- [MS15-049](#) Vulnerability in Silverlight Could Allow Elevation of Privilege (3058985)
- [MS15-048](#) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)
- [MS15-045](#) Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)
- [MS15-044](#) Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)
- [MS15-043](#) Cumulative Security Update for Internet Explorer (3049563)
- [MS15-041](#) Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)
- [MS15-039](#) Vulnerability in XML Core Services Could Allow Security Feature Bypass (3046482)
- [MS15-038](#) Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)
- [MS15-037](#) Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (3046269)
- [MS15-035](#) Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)
- [MS15-034](#) Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)
- [MS15-032](#) Cumulative Security Update for Internet Explorer (3038314)
- [MS15-031](#) Vulnerability in Schannel Could Allow Security Feature Bypass (3046049)
- [MS15-030](#) Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (3039976)
- [MS15-029](#) Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)
- [MS15-028](#) Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)
- [MS15-027](#) Vulnerability in NETLOGON Could Allow Spoofing (3002657)
- [MS15-025](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)
- [MS15-024](#) Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)



<http://buildings.honeywell.com/security>

<a href="#">MS15-023</a>	Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)
<a href="#">MS15-021</a>	Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)
<a href="#">MS15-020</a>	Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836)
<a href="#">MS15-018</a>	Cumulative Security Update for Internet Explorer (3032359)
<a href="#">MS15-016</a>	Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944)
<a href="#">MS15-015</a>	Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)
<a href="#">MS15-014</a>	Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)
<a href="#">MS15-011</a>	Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
<a href="#">MS15-010</a>	Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)
<a href="#">MS15-009</a>	Security Update for Internet Explorer (3034682)
<a href="#">MS15-008</a>	Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3019215)
<a href="#">MS15-007</a>	Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (3014029)
<a href="#">MS15-006</a>	Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (3004365)
<a href="#">MS15-005</a>	Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (3022777)
<a href="#">MS15-004</a>	Vulnerability in Windows Components Could Allow Elevation of Privilege (3025421)
<a href="#">MS15-003</a>	Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)
<a href="#">MS15-001</a>	Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266)

## **2014 – Microsoft® Patches Tested with Pro-Watch**

---

<a href="#">MS14-085</a>	Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3013126)
<a href="#">MS14-080</a>	Cumulative Security Update for Internet Explorer (3008923)
<a href="#">MS14-079</a>	Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)
<a href="#">MS14-076</a>	Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)
<a href="#">MS14-074</a>	Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)
<a href="#">MS14-072</a>	Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)
<a href="#">MS14-071</a>	Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)
<a href="#">MS14-068</a>	Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)
<a href="#">MS14-067</a>	Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)
<a href="#">MS14-066</a>	Vulnerability in Schannel Could Allow Remote Code Execution (2992611)
<a href="#">MS14-065</a>	Cumulative Security Update for Internet Explorer (3003057)
<a href="#">MS14-064</a>	Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)
<a href="#">MS14-060</a>	Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)
<a href="#">MS14-058</a>	Vulnerability in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)
<a href="#">MS14-057</a>	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)
<a href="#">MS14-056</a>	Cumulative Security Update for Internet Explorer (2987107)
<a href="#">MS14-053</a>	Vulnerability in .NET Framework Could Allow Denial of Service (2990931)
<a href="#">MS14-052</a>	Cumulative Security Update for Internet Explorer (2977629)
<a href="#">MS14-051</a>	Cumulative Security Update for Internet Explorer (2976627)

<http://buildings.honeywell.com/security>

<a href="#">MS14-049</a>	Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (2962490)
<a href="#">MS14-047</a>	Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)
<a href="#">MS14-046</a>	Vulnerability in .NET Framework Could Allow Security Feature Bypass (2984625)
<a href="#">MS14-045</a>	Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2984615)
<a href="#">MS14-044</a>	Vulnerabilities in SQL Server Could Allow Elevation of Privilege (2984340)
<a href="#">MS14-043</a>	Vulnerability in Windows Media Center Could Allow Remote Code Execution (2978742)
<a href="#">MS14-041</a>	Vulnerability in DirectShow Could Allow Elevation of Privilege (2975681)
<a href="#">MS14-040</a>	Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684)
<a href="#">MS14-039</a>	Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege (2975685)
<a href="#">MS14-038</a>	Vulnerability in Windows Journal Could Allow Remote Code Execution (2975689)
<a href="#">MS14-037</a>	Cumulative Security Update for Internet Explorer (2975687)
<a href="#">MS14-036</a>	Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (2967487)
<a href="#">MS14-035</a>	Cumulative Security Update for Internet Explorer (2969262)
<a href="#">MS14-033</a>	Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2966061)
<a href="#">MS14-031</a>	Vulnerability in TCP Protocol Could Allow Denial of Service (2962478)
<a href="#">MS14-030</a>	Vulnerability in Remote Desktop Could Allow Tampering (2969259)
<a href="#">MS14-029</a>	Security Update for Internet Explorer (2962482)
<a href="#">MS14-027</a>	Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)
<a href="#">MS14-026</a>	Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)
<a href="#">MS14-019</a>	Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2922229)
<a href="#">MS14-018</a>	Cumulative Security Update for Internet Explorer (2950467)
<a href="#">MS14-015</a>	Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2930275)
<a href="#">MS14-013</a>	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2929961)
<a href="#">MS14-012</a>	Cumulative Security Update for Internet Explorer (2925418)
<a href="#">MS14-011</a>	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)
<a href="#">MS14-010</a>	Cumulative Security Update for Internet Explorer (2909921)
<a href="#">MS14-009</a>	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607)
<a href="#">MS14-007</a>	Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)
<a href="#">MS14-005</a>	Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2916036)
<a href="#">MS14-003</a>	Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2913602)

## **2013 – Microsoft® Patches Tested with Pro-Watch**

---

<a href="#">MS13-101</a>	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)
<a href="#">MS13-099</a>	Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)
<a href="#">MS13-098</a>	Vulnerability in Windows Could Allow Remote Code Execution (2893294)
<a href="#">MS13-097</a>	Cumulative Security Update for Internet Explorer (2898785)
<a href="#">MS13-095</a>	Vulnerability in Digital Signatures Could Allow Denial of Service (2868626)
<a href="#">MS13-093</a>	Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

<http://buildings.honeywell.com/security>

- [MS13-090](#) Cumulative Security Update of ActiveX Kill Bits (2900986)
- [MS13-089](#) Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)
- [MS13-088](#) Cumulative Security Update for Internet Explorer (2888505)
- [MS13-083](#) Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)
- [MS13-082](#) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2878890)
- [MS13-081](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)
- [MS13-080](#) Cumulative Security Update for Internet Explorer (2879017)
- [MS13-077](#) Vulnerability in Windows Service Control Manager Could Allow Elevation of Privilege (2872339)
- [MS13-076](#) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2876315)
- [MS13-069](#) Cumulative Security Update for Internet Explorer (2870699)
- [MS13-065](#) Vulnerability in ICMPv6 could allow Denial of Service (2868623)
- [MS13-063](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2859537)
- [MS13-062](#) Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)
- [MS13-059](#) Cumulative Security Update for Internet Explorer (2862772)
- [MS13-058](#) Vulnerability in Windows Defender Could Allow Elevation of Privilege (2847927)
- [MS13-057](#) Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)
- [MS13-056](#) Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2845187)
- [MS13-055](#) Cumulative Security Update for Internet Explorer (2846071)
- [MS13-054](#) Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)
- [MS13-053](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)
- [MS13-052](#) Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)
- [MS13-050](#) Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege (2839894)
- [MS13-049](#) Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (2845690)
- [MS13-048](#) Vulnerability in Windows Kernel Could Allow Information Disclosure (2839229)
- [MS13-047](#) Cumulative Security Update for Internet Explorer (2838727)
- [MS13-046](#) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2840221)
- [MS13-040](#) Vulnerabilities in .NET Framework Could Allow Spoofing (2836440)
- [MS13-038](#) Security Update for Internet Explorer (2847204)
- [MS13-037](#) Cumulative Security Update for Internet Explorer (2829530)
- [MS13-036](#) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2829996)
- [MS13-033](#) Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2820917)
- [MS13-031](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)
- [MS13-029](#) Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)
- [MS13-028](#) Cumulative Security Update for Internet Explorer (2817183)
- [MS13-027](#) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)
- [MS13-021](#) Cumulative Security Update for Internet Explorer (2809289)
- [MS13-019](#) Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)

<http://buildings.honeywell.com/security>

- [MS13-018](#) Vulnerability in TCP/IP Could Allow Denial of Service (2790655)
- [MS13-017](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)
- [MS13-016](#) Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778344)
- [MS13-015](#) Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)
- [MS13-010](#) Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)
- [MS13-009](#) Cumulative Security Update for Internet Explorer (2792100)
- [MS13-008](#) Security Update for Internet Explorer (2799329)
- [MS13-007](#) Vulnerability in Open Data Protocol Could Allow Denial of Service (2769327)
- [MS13-006](#) Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)
- [MS13-005](#) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)
- [MS13-004](#) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)
- [MS13-002](#) Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)
- [MS13-001](#) Vulnerability in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)

## **2012 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS12-083](#) Vulnerability in IP-HTTPS Component Could Allow Security Feature Bypass (2765809)
- [MS12-082](#) Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)
- [MS12-081](#) Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)
- [MS12-078](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)
- [MS12-077](#) Cumulative Security Update for Internet Explorer (2761465)
- [MS12-075](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)
- [MS12-074](#) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)
- [MS12-073](#) Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure (2733829)
- [MS12-072](#) Vulnerabilities in Windows Shell Could Allow Remote Code Execution (2727528)
- [MS12-071](#) Cumulative Security Update for Internet Explorer (2761451)
- [MS12-070](#) Vulnerability in SQL Server Could Allow Elevation of Privilege (2754849)
- [MS12-069](#) Vulnerability in Kerberos Could Allow Denial of Service (2743555)
- [MS12-068](#) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)
- [MS12-063](#) Cumulative Security Update for Internet Explorer (2744842)
- [MS12-060](#) Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)
- [MS12-055](#) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)
- [MS12-054](#) Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)
- [MS12-053](#) Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)
- [MS12-052](#) Cumulative Security Update for Internet Explorer (2722913)
- [MS12-049](#) Vulnerability in TLS Could Allow Information Disclosure (2655992)
- [MS12-048](#) Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)
- [MS12-047](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)
- [MS12-045](#) Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)

<http://buildings.honeywell.com/security>

- [MS12-044](#) Cumulative Security Update for Internet Explorer (2719177)
- [MS12-043](#) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)
- [MS12-042](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)
- [MS12-041](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)
- [MS12-038](#) Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)
- [MS12-037](#) Cumulative Security Update for Internet Explorer (2699988)
- [MS12-036](#) Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)
- [MS12-035](#) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)
- [MS12-034](#) Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)
- [MS12-033](#) Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)
- [MS12-032](#) Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)
- [MS12-027](#) Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)
- [MS12-025](#) Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
- [MS12-024](#) Vulnerability in Windows Could Allow Remote Code Execution (2653956)
- [MS12-023](#) Cumulative Security Update for Internet Explorer (2675157)
- [MS12-020](#) Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
- [MS12-019](#) Vulnerability in DirectWrite Could Allow Denial of Service (2665364)
- [MS12-018](#) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)
- [MS12-016](#) Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)
- [MS12-014](#) Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637)
- [MS12-013](#) Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)
- [MS12-012](#) Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)
- [MS12-010](#) Cumulative Security Update for Internet Explorer (2647516)
- [MS12-009](#) Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)
- [MS12-008](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
- [MS12-006](#) Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)
- [MS12-005](#) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)
- [MS12-004](#) Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)
- [MS12-003](#) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524)
- [MS12-002](#) Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)
- [MS12-001](#) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)

## ***2011 – Microsoft® Patches Tested with Pro-Watch***

---

- [MS11-100](#) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
- [MS11-099](#) Cumulative Security Update for Internet Explorer (2618444)
- [MS11-098](#) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)
- [MS11-097](#) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)
- [MS11-093](#) Vulnerability in OLE Could Allow Remote Code Execution (2624667)

<http://buildings.honeywell.com/security>

- [MS11-092](#) Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)
- [MS11-090](#) Cumulative Security Update of ActiveX Kill Bits (2618451)
- [MS11-087](#) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)
- [MS11-085](#) Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)
- [MS11-084](#) Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)
- [MS11-083](#) Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)
- [MS11-081](#) Cumulative Security Update for Internet Explorer (2586448)
- [MS11-080](#) Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799)
- [MS11-078](#) Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)
- [MS11-077](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)
- [MS11-076](#) Vulnerability in Windows Media Center Could Allow Remote Code Execution (2604926)
- [MS11-075](#) Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)
- [MS11-071](#) Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)
- [MS11-069](#) Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)
- [MS11-068](#) Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)
- [MS11-066](#) Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943)
- [MS11-065](#) Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222)
- [MS11-064](#) Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)
- [MS11-063](#) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)
- [MS11-062](#) Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)
- [MS11-059](#) Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656)
- [MS11-057](#) Cumulative Security Update for Internet Explorer (2559049)
- [MS11-056](#) Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)
- [MS11-054](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)
- [MS11-053](#) Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220)
- [MS11-052](#) Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)
- [MS11-050](#) Cumulative Security Update for Internet Explorer (2530548)
- [MS11-049](#) Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893)
- [MS11-048](#) Vulnerability in SMB Server Could Allow Denial of Service (2536275)
- [MS11-046](#) Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)
- [MS11-044](#) Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)
- [MS11-043](#) Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)
- [MS11-042](#) Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)
- [MS11-041](#) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)
- [MS11-039](#) Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)
- [MS11-038](#) Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)
- [MS11-037](#) Vulnerability in MHTML Could Allow Information Disclosure (2544893)
- [MS11-035](#) Vulnerability in WINS Could Allow Remote Code Execution (2524426)

<http://buildings.honeywell.com/security>

- [MS11-034](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)
- [MS11-033](#) Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663)
- [MS11-032](#) Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)
- [MS11-031](#) Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)
- [MS11-030](#) Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)
- [MS11-029](#) Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)
- [MS11-028](#) Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)
- [MS11-027](#) Cumulative Security Update of ActiveX Kill Bits (2508272)
- [MS11-026](#) Vulnerability in MHTML Could Allow Information Disclosure (2503658)
- [MS11-024](#) Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)
- [MS11-020](#) Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)
- [MS11-019](#) Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)
- [MS11-018](#) Cumulative Security Update for Internet Explorer (2497640)
- [MS11-017](#) Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2508062)
- [MS11-015](#) Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)
- [MS11-014](#) Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960)
- [MS11-013](#) Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)
- [MS11-012](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)
- [MS11-011](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)
- [MS11-010](#) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2476687)
- [MS11-009](#) Vulnerability in JScript and VBScript Scripting Engines Could Allow Information Disclosure (2475792)
- [MS11-007](#) Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)
- [MS11-006](#) Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)
- [MS11-003](#) Cumulative Security Update for Internet Explorer (2482017)
- [MS11-002](#) Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)
- [MS11-001](#) Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935)

## **2010 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS10-102](#) Vulnerability in Hyper-V Could Allow Denial of Service (2345316)
- [MS10-101](#) Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)
- [MS10-100](#) Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)
- [MS10-099](#) Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)
- [MS10-098](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)
- [MS10-097](#) Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)
- [MS10-096](#) Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)
- [MS10-095](#) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)

<http://buildings.honeywell.com/security>

- [MS10-092](#) Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)
- [MS10-091](#) Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)
- [MS10-090](#) Cumulative Security Update for Internet Explorer (2416400)
- [MS10-085](#) Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)
- [MS10-084](#) Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937)
- [MS10-083](#) Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)
- [MS10-082](#) Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)
- [MS10-081](#) Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)
- [MS10-078](#) Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986)
- [MS10-077](#) Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)
- [MS10-076](#) Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)
- [MS10-075](#) Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)
- [MS10-074](#) Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)
- [MS10-073](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)
- [MS10-071](#) Cumulative Security Update for Internet Explorer (2360131)
- [MS10-070](#) Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)
- [MS10-069](#) Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546)
- [MS10-067](#) Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2259922)
- [MS10-066](#) Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802)
- [MS10-063](#) Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113)
- [MS10-062](#) Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)
- [MS10-061](#) Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)
- [MS10-060](#) Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)
- [MS10-059](#) Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)
- [MS10-058](#) Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)
- [MS10-055](#) Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)
- [MS10-054](#) Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)
- [MS10-053](#) Cumulative Security Update for Internet Explorer (2183461)
- [MS10-052](#) Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)
- [MS10-051](#) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)
- [MS10-050](#) Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)
- [MS10-049](#) Vulnerabilities in SChannel could allow Remote Code Execution (980436)
- [MS10-048](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)
- [MS10-047](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)
- [MS10-046](#) Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)
- [MS10-042](#) Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593)
- [MS10-041](#) Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)



<http://buildings.honeywell.com/security>

- [MS10-037](#) Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)
- [MS10-035](#) Cumulative Security Update for Internet Explorer (982381)
- [MS10-034](#) Cumulative Security Update of ActiveX Kill Bits (980195)
- [MS10-033](#) Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
- [MS10-032](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)
- [MS10-030](#) Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)
- [MS10-029](#) Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338)
- [MS10-026](#) Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)
- [MS10-025](#) Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858)
- [MS10-022](#) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)
- [MS10-021](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)
- [MS10-020](#) Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)
- [MS10-019](#) Vulnerabilities in Windows Could Allow Remote Code Execution (981210)
- [MS10-018](#) Cumulative Security Update for Internet Explorer (980182)
- [MS10-016](#) Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)
- [MS10-015](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)
- [MS10-014](#) Vulnerability in Kerberos Could Allow Denial of Service (977290)
- [MS10-013](#) Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)
- [MS10-012](#) Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)
- [MS10-011](#) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)
- [MS10-009](#) Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)
- [MS10-008](#) Cumulative Security Update of ActiveX Kill Bits (978262)
- [MS10-007](#) Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)
- [MS10-006](#) Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)
- [MS10-005](#) Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)
- [MS10-002](#) Cumulative Security Update for Internet Explorer (978207)
- [MS10-001](#) Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)

## **2009 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS09-073](#) Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)
- [MS09-072](#) Cumulative Security Update for Internet Explorer (976325)
- [MS09-071](#) Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)
- [MS09-069](#) Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)
- [MS09-065](#) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)
- [MS09-064](#) Vulnerability in License Logging Server Could Allow Remote Code Execution (974783)
- [MS09-063](#) Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565)
- [MS09-062](#) Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)
- [MS09-061](#) Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution

<http://buildings.honeywell.com/security>

(974378)

- [MS09-059](#) Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)
- [MS09-058](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)
- [MS09-057](#) Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)
- [MS09-056](#) Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)
- [MS09-055](#) Cumulative Security Update of ActiveX Kill Bits (973525)
- [MS09-054](#) Cumulative Security Update for Internet Explorer (974455)
- [MS09-052](#) Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112)
- [MS09-051](#) Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)
- [MS09-050](#) Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)
- [MS09-049](#) Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710)
- [MS09-048](#) Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)
- [MS09-047](#) Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812)
- [MS09-046](#) Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)
- [MS09-045](#) Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)
- [MS09-044](#) Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927)
- [MS09-043](#) Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)
- [MS09-042](#) Vulnerability in Telnet Could Allow Remote Code Execution (960859)
- [MS09-041](#) Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)
- [MS09-040](#) Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)
- [MS09-038](#) Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)
- [MS09-037](#) Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)
- [MS09-036](#) Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service (970957)
- [MS09-032](#) Cumulative Security Update of ActiveX Kill Bits (973346)
- [MS09-029](#) Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)
- [MS09-028](#) Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)
- [MS09-026](#) Vulnerability in RPC Could Allow Elevation of Privilege (970238)
- [MS09-025](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)
- [MS09-022](#) Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)
- [MS09-020](#) Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)
- [MS09-019](#) Cumulative Security Update for Internet Explorer (969897)
- [MS09-015](#) Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)
- [MS09-014](#) Cumulative Security Update for Internet Explorer (963027)
- [MS09-013](#) Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)
- [MS09-012](#) Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)
- [MS09-011](#) Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)
- [MS09-010](#) Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)
- [MS09-007](#) Vulnerability in SChannel Could Allow Spoofing (960225)

<http://buildings.honeywell.com/security>

- [MS09-006](#) Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)
- [MS09-004](#) Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)
- [MS09-002](#) Cumulative Security Update for Internet Explorer (961260)
- [MS09-001](#) Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

## **2008 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS08-078](#) Security Update for Internet Explorer (960714)
- [MS08-075](#) Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)
- [MS08-073](#) Cumulative Security Update for Internet Explorer (958215)
- [MS08-071](#) Vulnerabilities in GDI Could Allow Remote Code Execution (956802)
- [MS08-069](#) Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)
- [MS08-068](#) Vulnerability in SMB Could Allow Remote Code Execution (957097)
- [MS08-067](#) Vulnerability in Server Service Could Allow Remote Code Execution (958644)
- [MS08-066](#) Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803)
- [MS08-064](#) Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841)
- [MS08-063](#) Vulnerability in SMB Could Allow Remote Code Execution (957095)
- [MS08-062](#) Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155)
- [MS08-061](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211)
- [MS08-058](#) Cumulative Security Update for Internet Explorer (956390)
- [MS08-057](#) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (956416)
- [MS08-052](#) Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)
- [MS08-049](#) Vulnerabilities in Event System Could Allow Remote Code Execution (950974)
- [MS08-046](#) Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)
- [MS08-045](#) Cumulative Security Update for Internet Explorer (953838)
- [MS08-040](#) Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203)
- [MS08-037](#) Vulnerabilities in DNS Could Allow Spoofing (953230)
- [MS08-033](#) Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)
- [MS08-031](#) Cumulative Security Update for Internet Explorer (950759)
- [MS08-030](#) Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)
- [MS08-028](#) Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)
- [MS08-025](#) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)
- [MS08-024](#) Cumulative Security Update for Internet Explorer (947864)
- [MS08-023](#) Security Update of ActiveX Kill Bits (948881)
- [MS08-022](#) Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338)
- [MS08-021](#) Vulnerabilities in GDI Could Allow Remote Code Execution (948590)
- [MS08-020](#) Vulnerability in DNS Client Could Allow Spoofing (945553)
- [MS08-010](#) Cumulative Security Update for Internet Explorer (944533)

<http://buildings.honeywell.com/security>

- [MS08-008](#) Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)
- [MS08-007](#) Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)
- [MS08-002](#) Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)
- [MS08-001](#) Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)

## **2007 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS07-069](#) Cumulative Security Update for Internet Explorer (942615)
- [MS07-068](#) Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)
- [MS07-065](#) Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)
- [MS07-064](#) Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
- [MS07-062](#) Vulnerability in DNS Could Allow Spoofing (941672)
- [MS07-061](#) Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)
- [MS07-057](#) Cumulative Security Update for Internet Explorer (939653)
- [MS07-056](#) Security Update for Outlook Express and Windows Mail (941202)
- [MS07-055](#) Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)
- [MS07-051](#) Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)
- [MS07-050](#) Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
- [MS07-046](#) Vulnerability in GDI Could Allow Remote Code Execution (938829)
- [MS07-045](#) Cumulative Security Update for Internet Explorer (937143)
- [MS07-043](#) Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)
- [MS07-042](#) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)
- [MS07-041](#) Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)
- [MS07-040](#) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)
- [MS07-039](#) Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)
- [MS07-035](#) Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)
- [MS07-034](#) Cumulative Security Update for Outlook Express and Windows Mail (929123)
- [MS07-033](#) Cumulative Security Update for Internet Explorer (933566)
- [MS07-031](#) Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)
- [MS07-029](#) Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966)
- [MS07-027](#) Cumulative Security Update for Internet Explorer (931768)
- [MS07-022](#) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)
- [MS07-021](#) Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)
- [MS07-020](#) Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)
- [MS07-019](#) Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261)
- [MS07-017](#) Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
- [MS07-016](#) Cumulative Security Update for Internet Explorer (928090)
- [MS07-009](#) Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)
- [MS07-008](#) Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)

<http://buildings.honeywell.com/security>

[MS07-004](#) Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)

## **2006 – Microsoft® Patches Tested with Pro-Watch**

---

- [MS06-078](#) Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)
- [MS06-072](#) Cumulative Security Update for Internet Explorer (925454)
- [MS06-071](#) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (928088)
- [MS06-070](#) Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)
- [MS06-069](#) Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (923789)
- [MS06-068](#) Vulnerability in Microsoft Agent Could Allow Remote Code Execution (920213)
- [MS06-067](#) Cumulative Security Update for Internet Explorer (922760)
- [MS06-061](#) Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191)
- [MS06-057](#) Vulnerability in Windows Explorer Could Allow Remote Execution (923191)
- [MS06-048](#) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922968)
- [MS06-046](#) Vulnerability in HTML Help Could Allow Remote Code Execution (922616)
- [MS06-044](#) Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)
- [MS06-043](#) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (920214)
- [MS06-042](#) Cumulative Security Update for Internet Explorer (918899)
- [MS06-041](#) Vulnerabilities in DNS Resolution Could Allow Remote Code Execution (920683)
- [MS06-040](#) Vulnerability in Server Service Could Allow Remote Code Execution (921883)
- [MS06-039](#) Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (915384)
- [MS06-038](#) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (917284)
- [MS06-037](#) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (917285)
- [MS06-036](#) Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)
- [MS06-035](#) Vulnerability in Server Service Could Allow Remote Code Execution (917159)
- [MS06-025](#) Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280)
- [MS06-024](#) Vulnerability in Windows Media Player Could Allow Remote Code Execution (917734)
- [MS06-023](#) Vulnerability in Microsoft JScript Could Allow Remote Code Execution (917344)
- [MS06-022](#) Vulnerability in ART Image Rendering Could Allow Remote Code Execution (918439)
- [MS06-021](#) Cumulative Security Update for Internet Explorer (916281)
- [MS06-018](#) Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service (913580)
- [MS06-017](#) Vulnerability in Microsoft FrontPage 2002 Server Extensions could allow cross-site scripting
- [MS06-016](#) Cumulative Security Update for Outlook Express
- [MS06-015](#) Vulnerability in Windows Explorer Could Lead to Remote Code Execution
- [MS06-014](#) Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution
- [MS06-013](#) Cumulative security update for Internet Explorer
- [MS06-012](#) Vulnerabilities exist in Microsoft Office that could allow remote code execution.
- [MS06-011](#) Permissive Windows Services DACLs Could Allow Elevation of Privilege
- [MS06-010](#) Vulnerability in PowerPoint 2000 Could Allow Information Disclosure

<http://buildings.honeywell.com/security>

- [MS06-009](#) Vulnerability in the Korean Input Method Editor Could Allow Elevation of Privilege
- [MS06-008](#) Vulnerability in Web Client Service Could Allow Remote Code Execution
- [MS06-007](#) Vulnerability in TCP/IP Could Allow Denial of Service
- [MS06-006](#) Vulnerability in Windows Media Player plug-in with non-Microsoft Internet browsers could allow remote code execution
- [MS06-005](#) Vulnerability in Windows Media Player Could Allow Remote Code Execution
- [MS06-004](#) Cumulative security update for Internet Explorer
- [MS06-003](#) Vulnerability in TNEF decoding in Microsoft Outlook and Microsoft Exchange could allow remote code execution
- [MS06-002](#) Vulnerability in embedded Web fonts could allow remote code execution
- [MS06-001](#) Vulnerability in graphics rendering engine could allow remote code execution

## ***2005 – Microsoft® Patches Tested with Pro-Watch***

---

- [MS05-055](#) Vulnerability in Windows kernel could allow elevation of privilege
- [MS05-054](#) Cumulative security update for Internet Explorer
- [MS05-053](#) Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution
- [MS05-052](#) Cumulative security update for Internet Explorer
- [MS05-051](#) Vulnerabilities in MS DTC and COM+ could allow remote code execution
- [MS05-050](#) Vulnerability in DirectShow could allow remote code execution
- [MS05-049](#) Vulnerabilities in the Windows shell could allow for remote code execution
- [MS05-048](#) Vulnerability in the Microsoft Collaboration Data Objects could allow code execution
- [MS05-047](#) Vulnerability in Plug and Play could allow remote code execution and local elevation of privilege
- [MS05-046](#) Vulnerability in the Client Service for NetWare could allow remote code execution
- [MS05-045](#) Vulnerability in Network Connection Manager could allow denial of service
- [MS05-044](#) Vulnerability in the Windows FTP client could allow file transfer location tampering
- [MS05-043](#) Vulnerability in Print Spooler service could allow remote code execution
- [MS05-042](#) Vulnerabilities in Kerberos could allow denial of service, information disclosure, and spoofing
- [MS05-041](#) Vulnerability in Remote Desktop Protocol could allow denial of service
- [MS05-040](#) Vulnerability in Telephony service could allow remote code execution
- [MS05-039](#) Vulnerability in Plug and Play could allow remote code execution and elevation of privilege
- [MS05-038](#) Cumulative security update for Internet Explorer
- [MS05-037](#) Vulnerability in JView Profiler could allow remote code execution
- [MS05-036](#) Vulnerability in Microsoft Color Management Module could allow remote code execution
- [MS05-035](#) Vulnerability in Microsoft Word could allow remote code execution
- [MS05-034](#) Cumulative security update for Internet Security and Acceleration (ISA) Server 2000
- [MS05-033](#) Vulnerability in Telnet client could allow information disclosure
- [MS05-032](#) Vulnerability in Microsoft agent could allow spoofing
- [MS05-031](#) Vulnerability in step-by-step interactive training could allow remote code execution
- [MS05-030](#) Vulnerability in Outlook Express could allow remote code execution

<http://buildings.honeywell.com/security>

- [MS05-029](#) Vulnerability in Exchange Server 5.5 Outlook Web Access could allow cross-site scripting attacks
- [MS05-028](#) Vulnerability in the Web Client Service could allow remote code execution
- [MS05-027](#) Vulnerability in Server Message Block could allow remote code execution
- [MS05-026](#) Vulnerability in HTML Help could allow remote code execution
- [MS05-025](#) Cumulative security update for Internet Explorer
- [MS05-024](#) Vulnerability in Web View could allow remote code execution
- [MS05-023](#) Vulnerabilities in Microsoft Word May Lead to Remote Code Execution
- [MS05-022](#) Vulnerability in MSN Messenger Could Lead to Remote Code Execution
- [MS05-021](#) Vulnerability in Exchange Server Could Allow Remote Code Execution
- [MS05-020](#) Cumulative Security Update for Internet Explorer
- [MS05-019](#) Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service
- [MS05-018](#) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and Denial of Service
- [MS05-017](#) Vulnerability in Message Queuing Could Allow Code Execution
- [MS05-016](#) Vulnerability in Windows Shell that Could Allow Remote Code Execution
- [MS05-015](#) Vulnerability in hyperlink object library could allow remote code execution
- [MS05-014](#) Cumulative security update for Internet Explorer
- [MS05-013](#) Vulnerability in the DHTML editing component ActiveX control could allow code execution
- [MS05-012](#) Vulnerability in OLE and COM could allow remote code execution
- [MS05-011](#) Vulnerability in server message block could allow remote code execution
- [MS05-010](#) Vulnerability in the License Logging service could allow code execution
- [MS05-009](#) Vulnerability in PNG processing could lead to buffer overrun
- [MS05-008](#) Vulnerability in Windows shell could allow remote code execution
- [MS05-007](#) Vulnerability in Windows could allow information disclosure
- [MS05-006](#) Vulnerability in Windows SharePoint Services and SharePoint Team Services could allow cross-site scripting and spoofing attacks
- [MS05-005](#) Vulnerability in Microsoft Office XP could allow remote code execution
- [MS05-004](#) ASP.NET path validation vulnerability could allow unauthorized access
- [MS05-003](#) Vulnerability in Indexing Service Could Allow Remote Code Execution (871250)
- [MS05-002](#) Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)
- [MS05-001](#) Vulnerability in HTML Help Could Allow Remote Code Execution (890175)