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

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-2025-21409 patches not listed below are not applicable to a Pro-Watch system.

2025 – Microsoft® Patches Tested with Pro-Watch

Jan 2025:

CVE-2025-21409	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21374	Windows CSC Service Information Disclosure Vulnerability
CVE-2025-21340	Windows Virtualization-Based Security (VBS) Security Feature Bypass Vulnerability
CVE-2025-21339	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21334	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability
CVE-2025-21332	MapUrlToZone Security Feature Bypass Vulnerability
CVE-2025-21331	Windows Installer Elevation of Privilege Vulnerability
CVE-2025-21325	Windows Secure Kernel Mode Elevation of Privilege Vulnerability
CVE-2025-21324	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21317	Windows Kernel Memory Information Disclosure Vulnerability
CVE-2025-21312	Windows Smart Card Reader Information Disclosure Vulnerability
CVE-2025-21310	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21308	Windows Themes Spoofing Vulnerability
CVE-2025-21300	Windows upnphost.dll Denial of Service Vulnerability
CVE-2025-21292	Windows Search Service Elevation of Privilege Vulnerability
CVE-2025-21286	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21278	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2025-21276	Windows MapUrlToZone Denial of Service Vulnerability
CVE-2025-21261	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21246	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21245	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21232	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21229	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21228	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21227	Windows Digital Media Elevation of Privilege Vulnerability
CVE-2025-21223	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21217	Windows NTLM Spoofing Vulnerability
CVE-2025-21207	Windows Connected Devices Platform Service (Cdpsvc) Denial of Service Vulnerability
CVE-2025-21202	Windows Recovery Environment Agent Elevation of Privilege Vulnerability
CVE-2025-21193	Active Directory Federation Server Spoofing Vulnerability
CVE-2025-21189	MapUrlToZone Security Feature Bypass Vulnerability
CVE-2025-21176	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
CVE-2025-21409	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2025-21374	Windows CSC Service Information Disclosure Vulnerability
CVE-2025-21340	Windows Virtualization-Based Security (VBS) Security Feature Bypass Vulnerability
CVE-2025-21339	Windows Telephony Service Remote Code Execution Vulnerability

2024 – Microsoft® Patches Tested with Pro-Watch

Dec 2024:

CVE-2024-49138	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-49128	Windows Remote Desktop Services Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-49127	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2024-49125	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-49118	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability
CVE-2024-49116	Windows Remote Desktop Services Remote Code Execution Vulnerability
CVE-2024-49114	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2024-49113	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
CVE-2024-49112	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2024-49110	Windows Mobile Broadband Driver Elevation of Privilege Vulnerability
CVE-2024-49109	Wireless Wide Area Network Service (WwanSvc) Elevation of Privilege Vulnerability
CVE-2024-49108	Windows Remote Desktop Services Remote Code Execution Vulnerability
CVE-2024-49107	WmsRepair Service Elevation of Privilege Vulnerability
CVE-2024-49105	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2024-49095	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
CVE-2024-49091	Windows Domain Name Service Remote Code Execution Vulnerability
CVE-2024-49090	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-49088	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-49082	Windows File Explorer Information Disclosure Vulnerability
CVE-2024-49081	Wireless Wide Area Network Service (WwanSvc) Elevation of Privilege Vulnerability
CVE-2024-49080	Windows IP Routing Management Snapin Remote Code Execution Vulnerability
CVE-2024-49079	Input Method Editor (IME) Remote Code Execution Vulnerability
CVE-2024-49076	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability
CVE-2024-49075	Windows Remote Desktop Services Denial of Service Vulnerability
CVE-2024-49043	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability
CVE-2024-49021	Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2024-49018	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49017	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49016	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49015	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49014	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49013	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49012	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49011	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49010	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49009	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49008	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49007	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49006	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49005	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49004	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49003	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49002	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49001	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49000	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48999	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48998	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48997	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48996	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48995	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48993	SQL Server Native Client Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

Nov 2024:

CVE-2024-49043	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability
CVE-2024-49039	Windows Task Scheduler Elevation of Privilege Vulnerability
CVE-2024-49021	Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2024-49019	Active Directory Certificate Services Elevation of Privilege Vulnerability
CVE-2024-49018	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49017	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49016	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49015	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49014	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49013	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49012	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49011	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49010	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49009	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49008	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49007	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49006	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49005	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49004	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49003	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49002	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49001	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-49000	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48999	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48998	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48997	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48996	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48995	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48994	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-48993	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-43644	Windows Client-Side Caching Elevation of Privilege Vulnerability
CVE-2024-43642	Windows SMB Denial of Service Vulnerability
CVE-2024-43641	Windows Registry Elevation of Privilege Vulnerability
CVE-2024-43640	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
CVE-2024-43639	Windows KDC Proxy Remote Code Execution Vulnerability
CVE-2024-43636	Win32k Elevation of Privilege Vulnerability
CVE-2024-43635	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2024-43630	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-43629	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-43626	Windows Telephony Service Elevation of Privilege Vulnerability
CVE-2024-43622	Windows Telephony Service Remote Code Execution Vulnerability
CVE-2024-43462	SQL Server Native Client Remote Code Execution Vulnerability
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability
CVE-2024-38203	Windows Package Library Manager Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

Oct 2024:

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

Sep 2024:

CVE-2024-43487	Windows Mark of the Web Security Feature Bypass Vulnerability
CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability
CVE-2024-43458	Windows Networking Information Disclosure Vulnerability
CVE-2024-43455	Windows Remote Desktop Licensing Service Spoofing Vulnerability
CVE-2024-43454	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38263	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38260	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38259	Microsoft Management Console Remote Code Execution Vulnerability
CVE-2024-38258	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability
CVE-2024-38257	Microsoft AllJoyn API Information Disclosure Vulnerability
CVE-2024-38249	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2024-38248	Windows Storage Elevation of Privilege Vulnerability
CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-38246	Win32k Elevation of Privilege Vulnerability
CVE-2024-38245	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
CVE-2024-38244	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
CVE-2024-38243	Kernel Streaming Service Driver Elevation of Privilege Vulnerability
CVE-2024-38239	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2024-38237	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38235	Windows Hyper-V Denial of Service Vulnerability
CVE-2024-38119	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability
CVE-2024-38045	Windows TCP/IP Remote Code Execution Vulnerability
CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability
CVE-2024-37980	Microsoft SQL Server Elevation of Privilege Vulnerability
CVE-2024-37966	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
CVE-2024-37965	Microsoft SQL Server Elevation of Privilege Vulnerability
CVE-2024-37342	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
CVE-2024-37341	Microsoft SQL Server Elevation of Privilege Vulnerability
CVE-2024-37340	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-37339	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-37338	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-37337	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability
CVE-2024-37335	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-30073	Windows Security Zone Mapping Security Feature Bypass Vulnerability
CVE-2024-26191	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-26186	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability
CVE-2024-21416	Windows TCP/IP Remote Code Execution Vulnerability

Aug 2024:

CVE-2024-38223	Windows Initial Machine Configuration Elevation of Privilege Vulnerability
CVE-2024-38215	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2024-38214	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
CVE-2024-38199	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability
CVE-2024-38193	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2024-38180	Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2024-38178	Scripting Engine Memory Corruption Vulnerability
CVE-2024-38155	Security Center Broker Information Disclosure Vulnerability
CVE-2024-38154	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-38153	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-38152	Windows OLE Remote Code Execution Vulnerability
CVE-2024-38151	Windows Kernel Information Disclosure Vulnerability
CVE-2024-38150	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-38148	Windows Secure Channel Denial of Service Vulnerability
CVE-2024-38147	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-38146	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38143	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
CVE-2024-38140	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability
CVE-2024-38134	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-38127	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2024-38122	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability
CVE-2024-38120	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-38117	NTFS Elevation of Privilege Vulnerability
CVE-2024-38106	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-37968	Windows DNS Spoofing Vulnerability
CVE-2022-3775	Redhat: CVE-2022-3775 grub2 - Heap based out-of-bounds write when rendering certain Unicode seq

July 2024:

CVE-2024-39379	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2024-38176	GroupMe Elevation of Privilege Vulnerability
CVE-2024-38164	GroupMe Elevation of Privilege Vulnerability
CVE-2024-38156	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2024-38103	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38095	.NET and Visual Studio Denial of Service Vulnerability
CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
CVE-2024-38073	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38070	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2024-38068	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability
CVE-2024-38065	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38058	BitLocker Security Feature Bypass Vulnerability
CVE-2024-38057	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38057	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
CVE-2024-38049	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability
CVE-2024-38047	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38047	PowerShell Elevation of Privilege Vulnerability
CVE-2024-38044	DHCP Server Service Remote Code Execution Vulnerability
CVE-2024-38030	Windows Themes Spoofing Vulnerability
CVE-2024-38027	Windows Line Printer Daemon Service Denial of Service Vulnerability
CVE-2024-38017	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-38011	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38011	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38010	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37989	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37989	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37988	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37984	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-37334	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-30105	.NET Core and Visual Studio Denial of Service Vulnerability
CVE-2024-7005	Chromium: CVE-2024-7005 Insufficient validation of untrusted input in Safe Browsing
CVE-2024-7004	Chromium: CVE-2024-7004 Insufficient validation of untrusted input in Safe Browsing
CVE-2024-7003	Chromium: CVE-2024-7003 Inappropriate implementation in FedCM
CVE-2024-7001	Chromium: CVE-2024-7001 Inappropriate implementation in HTML
CVE-2024-7000	Chromium: CVE-2024-7000 Use after free in CSS
CVE-2024-6999	Chromium: CVE-2024-6999 Inappropriate implementation in FedCM
CVE-2024-6998	Chromium: CVE-2024-6998 Use after free in User Education
CVE-2024-6997	Chromium: CVE-2024-6997 Use after free in Tabs
CVE-2024-6996	Chromium: CVE-2024-6996 Race in Frames
CVE-2024-6995	Chromium: CVE-2024-6995 Inappropriate implementation in Fullscreen
CVE-2024-6994	Chromium: CVE-2024-6994 Heap buffer overflow in Layout
CVE-2024-6993	Chromium: CVE-2024-6993
CVE-2024-6992	Chromium: CVE-2024-6992
CVE-2024-6991	Chromium: CVE-2024-6991 Use after free in Dawn
CVE-2024-6989	Chromium: CVE-2024-6989 Use after free in Loader
CVE-2024-6988	Chromium: CVE-2024-6988 Use after free in Downloads
CVE-2024-6779	Chromium: CVE-2024-6779 Out of bounds memory access in V8
CVE-2024-6778	Chromium: CVE-2024-6778 Race in DevTools
CVE-2024-6777	Chromium: CVE-2024-6777 Use after free in Navigation
CVE-2024-6776	Chromium: CVE-2024-6776 Use after free in Audio
CVE-2024-6775	Chromium: CVE-2024-6775 Use after free in Media Stream
CVE-2024-6774	Chromium: CVE-2024-6774 Use after free in Screen Capture
CVE-2024-6773	Chromium: CVE-2024-6773 Type Confusion in V8
CVE-2024-6772	Chromium: CVE-2024-6772 Inappropriate implementation in V8
CVE-2024-6387	RedHat Openssh: CVE-2024-6387 Remote Code Execution Due To A Race Condition In Signal Handlir

June 2024:

CVE-2024-39684	Github: CVE-2024-39684 TenCent RapidJSON Elevation of Privilege Vulnerability
CVE-2024-38105	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38101	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2024-38078	Xbox Wireless Adapter Remote Code Execution Vulnerability
CVE-2024-38076	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability
CVE-2024-38073	Windows Remote Desktop Licensing Service Denial of Service Vulnerability
CVE-2024-38070	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2024-38068	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability
CVE-2024-38065	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-38058	BitLocker Security Feature Bypass Vulnerability
CVE-2024-38057	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
CVE-2024-38052	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

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

May 2024:

CVE-2024-30051	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-30050	Windows Mark of the Web Security Feature Bypass Vulnerability
CVE-2024-30049	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2024-30040	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2024-30039	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-30038	Win32k Elevation of Privilege Vulnerability
CVE-2024-30037	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-30036	Windows Deployment Services Information Disclosure Vulnerability
CVE-2024-30035	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-30034	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
CVE-2024-30033	Windows Search Service Elevation of Privilege Vulnerability
CVE-2024-30032	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2024-30031	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2024-30029	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30028	Win32k Elevation of Privilege Vulnerability
CVE-2024-30027	NTFS Elevation of Privilege Vulnerability
CVE-2024-30025	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-30024	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30023	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-30022	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30021	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30020	Windows Cryptographic Services Remote Code Execution Vulnerability
CVE-2024-30019	DHCP Server Service Denial of Service Vulnerability
CVE-2024-30018	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-30017	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2024-30016	Windows Cryptographic Services Information Disclosure Vulnerability
CVE-2024-30015	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30014	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30012	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30011	Windows Hyper-V Denial of Service Vulnerability
CVE-2024-30010	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2024-30009	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-30008	Windows DWM Core Library Information Disclosure Vulnerability
CVE-2024-30006	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-30005	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30004	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30003	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30002	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30001	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-30000	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-29999	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-29998	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-29997	Windows Mobile Broadband Driver Remote Code Execution Vulnerability
CVE-2024-29996	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2024-29994	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability
CVE-2024-29984	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-29983	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-29046	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-29045	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-29044	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28945	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28944	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28943	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28941	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28940	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28939	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28938	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28937	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28935	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28934	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28933	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28931	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28930	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28929	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

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

April 2024:

CVE-2024-29988	SmartScreen Prompt Security Feature Bypass Vulnerability
CVE-2024-29066	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
CVE-2024-29064	Windows Hyper-V Denial of Service Vulnerability
CVE-2024-29062	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-29061	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-29056	Windows Authentication Elevation of Privilege Vulnerability
CVE-2024-29052	Windows Storage Elevation of Privilege Vulnerability
CVE-2024-29050	Windows Cryptographic Services Remote Code Execution Vulnerability
CVE-2024-29044	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-29043	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28943	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28941	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28938	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28937	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28936	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28935	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-28934	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28933	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28932	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28931	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28930	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28929	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVE-2024-28925	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28924	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28923	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28922	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28921	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28920	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28919	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28903	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28902	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-28901	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-28900	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-28898	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28897	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-28896	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26255	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-26254	Microsoft Virtual Machine Bus (VMBus) Denial of Service Vulnerability
CVE-2024-26253	sys Remote Code Execution Vulnerability
CVE-2024-26252	Windows rndismp6.sys Remote Code Execution Vulnerability
CVE-2024-26252	sys Remote Code Execution Vulnerability
CVE-2024-26250	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26248	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2024-26244	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-26243	Windows USB Print Driver Elevation of Privilege Vulnerability
CVE-2024-26242	Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2024-26241	Win32k Elevation of Privilege Vulnerability
CVE-2024-26240	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26239	Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2024-26237	Windows Defender Credential Guard Elevation of Privilege Vulnerability
CVE-2024-26234	Proxy Driver Spoofing Vulnerability
CVE-2024-26233	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26232	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability
CVE-2024-26231	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26230	Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2024-26229	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2024-26228	Windows Cryptographic Services Security Feature Bypass Vulnerability
CVE-2024-26227	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26226	Windows Distributed File System (DFS) Information Disclosure Vulnerability
CVE-2024-26224	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26223	Windows DNS Server Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-26222	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26221	Windows DNS Server Remote Code Execution Vulnerability
CVE-2024-26220	Windows Mobile Hotspot Information Disclosure Vulnerability
CVE-2024-26219	sys Denial of Service Vulnerability
CVE-2024-26218	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-26217	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-26216	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2024-26215	DHCP Server Service Denial of Service Vulnerability
CVE-2024-26214	Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability
CVE-2024-26212	DHCP Server Service Denial of Service Vulnerability
CVE-2024-26211	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2024-26210	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-26209	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
CVE-2024-26208	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability
CVE-2024-26207	Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2024-26205	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-26202	DHCP Server Service Remote Code Execution Vulnerability
CVE-2024-26200	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-26195	DHCP Server Service Remote Code Execution Vulnerability
CVE-2024-26194	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26189	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26183	Windows Kerberos Denial of Service Vulnerability
CVE-2024-26180	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26179	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2024-26175	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26172	Windows DWM Core Library Information Disclosure Vulnerability
CVE-2024-26171	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26168	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-26158	Microsoft Install Service Elevation of Privilege Vulnerability
CVE-2024-23594	Stack buffer overflow in Lenovo system recovery boot manager
CVE-2024-23593	Zero Out Boot Manager and drop to UEFI Shell
CVE-2024-23593	Lenovo: CVE-2024-23593 Zero Out Boot Manager and drop to UEFI Shell
CVE-2024-21447	Windows Authentication Elevation of Privilege Vulnerability
CVE-2024-21409	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
CVE-2024-21409	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability
CVE-2024-20693	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-20689	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-20688	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-20678	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2024-20669	Secure Boot Security Feature Bypass Vulnerability
CVE-2024-20665	BitLocker Security Feature Bypass Vulnerability
CVE-2022-0001	Branch History Injection
CVE-2022-0001	Intel: CVE-2022-0001 Branch History Injection

CVE-2024-29049	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-29981	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2024-29986	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability
CVE-2024-29987	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2024-29991	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
CVE-2024-3156	Chromium CVE-2024-3156 Inappropriate implementation in V8
CVE-2024-3157	Chromium CVE-2024-3157 Out of bounds write in Compositing
CVE-2024-3158	Chromium CVE-2024-3158 Use after free in Bookmarks
CVE-2024-3159	Chromium CVE-2024-3159 Out of bounds memory access in V8
CVE-2024-3515	Chromium CVE-2024-3515 Use after free in Dawn
CVE-2024-3516	Chromium CVE-2024-3516 Heap buffer overflow in ANGLE
CVE-2024-3832	Chromium CVE-2024-3832 Object corruption in V8
CVE-2024-3833	Chromium CVE-2024-3833 Object corruption in WebAssembly
CVE-2024-3834	Chromium CVE-2024-3834 Use after free in Downloads
CVE-2024-3837	Chromium CVE-2024-3837 Use after free in QUIC
CVE-2024-3838	Chromium CVE-2024-3838 Inappropriate implementation in Autofill
CVE-2024-3839	Chromium CVE-2024-3839 Out of bounds read in Fonts
CVE-2024-3840	Chromium CVE-2024-3840 Insufficient policy enforcement in Site Isolation
CVE-2024-3841	Chromium CVE-2024-3841 Insufficient data validation in Browser Switcher
CVE-2024-3843	Chromium CVE-2024-3843 Insufficient data validation in Downloads
CVE-2024-3844	Chromium CVE-2024-3844 Inappropriate implementation in Extensions
CVE-2024-3845	Chromium CVE-2024-3845 Inappropriate implementation in Network
CVE-2024-3846	Chromium CVE-2024-3846 Inappropriate implementation in Prompts
CVE-2024-3847	Chromium CVE-2024-3847 Insufficient policy enforcement in WebUI
CVE-2024-3914	Chromium CVE-2024-3914 Use after free in V8

March 2024:

CVE-2024-26197	Windows Standards-Based Storage Management Service Denial of Service Vulnerability
CVE-2024-26190	Microsoft QUIC Denial of Service Vulnerability
CVE-2024-26182	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-26181	Windows Kernel Denial of Service Vulnerability
CVE-2024-26178	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-26177	Windows Kernel Information Disclosure Vulnerability
CVE-2024-26176	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-26174	Windows Kernel Information Disclosure Vulnerability
CVE-2024-26173	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-26170	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability
CVE-2024-26169	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2024-26166	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-26162	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2024-26161	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-26160	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
CVE-2024-26159	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2024-21451	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2024-21450	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2024-21446	NTFS Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

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
CVE-2023-50387	NSSEC verification complexity can be exploited to exhaust CPU resources and stall DNS resolvers
CVE-2023-50387	MITRE: CVE-2023-50387 DNSSEC verification complexity can be exploited to exhaust CPU resource DNS resolvers
CVE-2024-26192	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2024-21423	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2024-21399	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2024-1676	Chromium CVE-2024-1676 Inappropriate implementation in Navigation

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

http://buildings.honeywell.com/security

CVE-2024-1675	Chromium CVE-2024-1675 Insufficient policy enforcement in Download
CVE-2024-1674	Chromium CVE-2024-1674 Inappropriate implementation in Navigation
CVE-2024-1673	Chromium CVE-2024-1673 Use after free in Accessibility
CVE-2024-1672	Chromium CVE-2024-1672 Inappropriate implementation in Content Security Policy
CVE-2024-1671	Chromium CVE-2024-1671 Inappropriate implementation in Site Isolation
CVE-2024-1670	Chromium CVE-2024-1670 Use after free in Mojo
CVE-2024-1669	Chromium CVE-2024-1669 Out of bounds memory access in Blink
CVE-2024-1284	Chromium CVE-2024-1284 Use after free in Mojo
CVE-2024-1283	Chromium CVE-2024-1283 Heap buffer overflow in Skia
CVE-2024-1077	Chromium CVE-2024-1077 Use after free in Network
CVE-2024-1060	Chromium CVE-2024-1060 Use after free in Canvas

January 2024:

CVE-2024-21320	Windows Themes Spoofing Vulnerability
CVE-2024-21316	No Vulnerability Name Found
CVE-2024-21314	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-21313	Windows TCP/IP Information Disclosure Vulnerability
CVE-2024-21312	NET Framework Denial of Service Vulnerability
CVE-2024-21311	Windows Cryptographic Services Information Disclosure Vulnerability
CVE-2024-21310	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2024-21309	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
CVE-2024-21307	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2024-21306	Microsoft Bluetooth Driver Spoofing Vulnerability
CVE-2024-21305	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability
CVE-2024-20700	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2024-20699	Windows Hyper-V Denial of Service Vulnerability
CVE-2024-20698	Windows Kernel Elevation of Privilege Vulnerability
CVE-2024-20697	Windows Libarchive Remote Code Execution Vulnerability
CVE-2024-20696	Windows Libarchive Remote Code Execution Vulnerability
CVE-2024-20694	Windows CoreMessaging Information Disclosure Vulnerability
CVE-2024-20692	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
CVE-2024-20691	Windows Themes Information Disclosure Vulnerability
CVE-2024-20690	Windows Nearby Sharing Spoofing Vulnerability
CVE-2024-20687	Microsoft AllJoyn API Denial of Service Vulnerability
CVE-2024-20683	Win32k Elevation of Privilege Vulnerability
CVE-2024-20682	Windows Cryptographic Services Remote Code Execution Vulnerability
CVE-2024-20681	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2024-20680	No Vulnerability Name Found
CVE-2024-20674	Windows Kerberos Security Feature Bypass Vulnerability
CVE-2024-20666	BitLocker Security Feature Bypass Vulnerability
CVE-2024-20664	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-20663	No Vulnerability Name Found
CVE-2024-20662	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability
CVE-2024-20661	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2024-20660	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2024-20658	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2024-20657	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2024-20655	Microsoft Online Certificate Status Protocol (OCSP) Remote Code Execution Vulnerability
CVE-2024-20654	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2024-20653	Microsoft Common Log File System Elevation of Privilege Vulnerability
CVE-2024-20652	Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2024-0057	NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability
CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vul

December 2023:

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

November 2023:

CVE-2023-36719	Microsoft Speech Application Programming Interface (SAPI) Elevation of Privilege Vulnerability
CVE-2023-36705	Windows Installer Elevation of Privilege Vulnerability
CVE-2023-36560	NET Security Feature Bypass Vulnerability
CVE-2023-36428	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
CVE-2023-36427	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2023-36425	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
CVE-2023-36424	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-36423	Microsoft Remote Registry Service Remote Code Execution Vulnerability
CVE-2023-36408	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2023-36407	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2023-36406	Windows Hyper-V Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-36405	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36404	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36403	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36402	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-36401	Microsoft Remote Registry Service Remote Code Execution Vulnerability
CVE-2023-36400	Windows HMAC Key Derivation Elevation of Privilege Vulnerability
CVE-2023-36399	Windows Storage Elevation of Privilege Vulnerability
CVE-2023-36398	Windows NTFS Information Disclosure Vulnerability
CVE-2023-36397	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-36395	Windows Deployment Services Denial of Service Vulnerability
CVE-2023-36394	Windows Search Service Elevation of Privilege Vulnerability
CVE-2023-36393	Windows User Interface Application Core Remote Code Execution Vulnerability
CVE-2023-36392	DHCP Server Service Denial of Service Vulnerability
CVE-2023-36049	No Vulnerability Name Found
CVE-2023-36047	Windows Authentication Elevation of Privilege Vulnerability
CVE-2023-36046	Windows Authentication Denial of Service Vulnerability
CVE-2023-36036	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-36033	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2023-36028	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerabili
CVE-2023-36025	Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2023-36017	Windows Scripting Engine Memory Corruption Vulnerability
CVE-2023-24023	Mitre CVE-2023-24023 Bluetooth Vulnerability

CVE-2023-36008	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-36014	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-36022	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-36024	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-36026	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2023-36027	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-36034	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-5480	Chromium CVE-2023-5480 Inappropriate implementation in Payments
CVE-2023-5482	Chromium CVE-2023-5482 Insufficient data validation in USB
CVE-2023-5849	Chromium CVE-2023-5849 Integer overflow in USB
CVE-2023-5850	Chromium CVE-2023-5850 Incorrect security UI in Downloads
CVE-2023-5851	Chromium CVE-2023-5851 Inappropriate implementation in Downloads
CVE-2023-5852	Chromium CVE-2023-5852 Use after free in Printing
CVE-2023-5853	Chromium CVE-2023-5853 Incorrect security UI in Downloads
CVE-2023-5854	Chromium CVE-2023-5854 Use after free in Profiles
CVE-2023-5855	Chromium CVE-2023-5855 Use after free in Reading Mode
CVE-2023-5856	Chromium CVE-2023-5856 Use after free in Side Panel
CVE-2023-5857	Chromium CVE-2023-5857 Inappropriate implementation in Downloads
CVE-2023-5858	Chromium CVE-2023-5858 Inappropriate implementation in WebApp Provider
CVE-2023-5859	Chromium CVE-2023-5859 Incorrect security UI in Picture In Picture
CVE-2023-5996	Chromium CVE-2023-5996 Use after free in WebAudio
CVE-2023-5997	Chromium CVE-2023-5997 Use after free in Garbage Collection

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

http://buildings.honeywell.com/security

CVE-2023-6112	Chromium CVE-2023-6112 Use after free in Navigation
CVE-2023-44487	HTTP/2 protocol allows a denial of service
CVE-2023-41774	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41773	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41772	Win32k Elevation of Privilege Vulnerability
CVE-2023-41771	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41770	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41769	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41768	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41767	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-41766	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
CVE-2023-41765	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-38171	Microsoft QUIC Denial of Service Vulnerability
CVE-2023-38166	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-38159	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-36902	Windows Runtime Remote Code Execution Vulnerability
CVE-2023-36776	Win32k Elevation of Privilege Vulnerability
CVE-2023-36743	Win32k Elevation of Privilege Vulnerability
CVE-2023-36732	Win32k Elevation of Privilege Vulnerability
CVE-2023-36731	Win32k Elevation of Privilege Vulnerability
CVE-2023-36729	Named Pipe File System Elevation of Privilege Vulnerability
CVE-2023-36726	Windows Internet Key Exchange (IKE) Extension Elevation of Privilege Vulnerability
CVE-2023-36725	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36724	Windows Power Management Service Information Disclosure Vulnerability
CVE-2023-36723	Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2023-36722	Active Directory Domain Services Information Disclosure Vulnerability
CVE-2023-36721	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2023-36720	Windows Mixed Reality Developer Tools Denial of Service Vulnerability
CVE-2023-36718	Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability
CVE-2023-36717	Windows Virtual Trusted Platform Module Denial of Service Vulnerability
CVE-2023-36713	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2023-36712	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36711	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability
CVE-2023-36710	Windows Media Foundation Core Remote Code Execution Vulnerability
CVE-2023-36709	Microsoft AllJoyn API Denial of Service Vulnerability
CVE-2023-36707	Windows Deployment Services Denial of Service Vulnerability
CVE-2023-36706	Windows Deployment Services Information Disclosure Vulnerability
CVE-2023-36704	Windows Setup Files Cleanup Remote Code Execution Vulnerability
CVE-2023-36703	DHCP Server Service Denial of Service Vulnerability
CVE-2023-36702	Microsoft DirectMusic Remote Code Execution Vulnerability
CVE-2023-36701	Microsoft Resilient File System (ReFS) Elevation of Privilege Vulnerability
CVE-2023-36698	Windows Kernel Security Feature Bypass Vulnerability
CVE-2023-36697	Microsoft Message Queuing Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-36606	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-36605	Windows Named Pipe Filesystem Elevation of Privilege Vulnerability
CVE-2023-36603	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-36602	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-36598	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability
CVE-2023-36596	Remote Procedure Call Information Disclosure Vulnerability
CVE-2023-36594	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-36593	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36592	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36591	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36590	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36589	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36585	Active Template Library Denial of Service Vulnerability
CVE-2023-36584	Windows Mark of the Web Security Feature Bypass Vulnerability
CVE-2023-36583	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36582	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36581	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-36579	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-36578	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36577	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-36576	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36575	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36574	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36573	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36572	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36571	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36570	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36567	Windows Deployment Services Information Disclosure Vulnerability
CVE-2023-36564	Windows Search Security Feature Bypass Vulnerability
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability
CVE-2023-36557	PrintHTML API Remote Code Execution Vulnerability
CVE-2023-36438	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-36436	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2023-36435	Microsoft QUIC Denial of Service Vulnerability
CVE-2023-36434	Windows IIS Server Elevation of Privilege Vulnerability
CVE-2023-36431	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-35349	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-29348	Windows Remote Desktop Gateway (RD Gateway) Information Disclosure Vulnerability

CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability
CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability
CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability
CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability
CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-38150	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability
CVE-2023-38146	Windows Themes Remote Code Execution Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability

CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-5346	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)

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

http://buildings.honeywell.com/security

CVE-2023-4078	Chromium: CVE-2023-4078 Inappropriate implementation in Extensions
CVE-2023-4077	Chromium: CVE-2023-4077 Insufficient data validation in Extensions
CVE-2023-4076	Chromium: CVE-2023-4076 Use after free in WebRTC
CVE-2023-4075	Chromium: CVE-2023-4075 Use after free in Cast
CVE-2023-4074	Chromium: CVE-2023-4074 Use after free in Blink Task Scheduling
CVE-2023-4073	Chromium: CVE-2023-4073 Out of bounds memory access in ANGLE
CVE-2023-4072	Chromium: CVE-2023-4072 Out of bounds read and write in WebGL
CVE-2023-4071	Chromium: CVE-2023-4071 Heap buffer overflow in Visuals
CVE-2023-4070	Chromium: CVE-2023-4070 Type Confusion in V8
CVE-2023-4069	Chromium: CVE-2023-4069 Type Confusion in V8
CVE-2023-4068	Chromium: CVE-2023-4068 Type Confusion in V8
CVE-2023-38254	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-38186	Windows Mobile Device Management Elevation of Privilege Vulnerability
CVE-2023-38184	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2023-38172	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-38157	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
CVE-2023-38154	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-36914	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability
CVE-2023-36913	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2023-36912	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-36911	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36910	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-36909	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-36908	Windows Hyper-V Information Disclosure Vulnerability
CVE-2023-36907	Windows Cryptographic Services Information Disclosure Vulnerability
CVE-2023-36906	Windows Cryptographic Services Information Disclosure Vulnerability
CVE-2023-36905	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability
CVE-2023-36904	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-36903	Windows System Assessment Tool Elevation of Privilege Vulnerability
CVE-2023-36900	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-36898	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability
CVE-2023-36889	Windows Group Policy Security Feature Bypass Vulnerability
CVE-2023-36882	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-35387	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability
CVE-2023-35386	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35385	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-35384	Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2023-35383	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2023-35382	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35381	Windows Fax Service Remote Code Execution Vulnerability
CVE-2023-35380	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35378	Windows Projected File System Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-35377	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-35376	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-35359	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35316	Remote Procedure Call Runtime Information Disclosure Vulnerability
CVE-2023-20569	This may result in speculative execution at an attacker-controlled address
CVE-2023-38187	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-3740	Chromium: CVE-2023-3740 Insufficient validation of untrusted input in Themes
CVE-2023-3738	Chromium: CVE-2023-3738 Inappropriate implementation in Autofill
CVE-2023-3737	Chromium: CVE-2023-3737 Inappropriate implementation in Notifications
CVE-2023-3736	Chromium: CVE-2023-3736 Inappropriate implementation in Custom Tabs
CVE-2023-3735	Chromium: CVE-2023-3735 Inappropriate implementation in Web API Permission Prompts
CVE-2023-3734	Chromium: CVE-2023-3734 Inappropriate implementation in Picture In Picture
CVE-2023-3733	Chromium: CVE-2023-3733 Inappropriate implementation in WebApp Installs
CVE-2023-3732	Chromium: CVE-2023-3732 Out of bounds memory access in Mojo
CVE-2023-3730	Chromium: CVE-2023-3730 Use after free in Tab Groups
CVE-2023-3728	Chromium: CVE-2023-3728 Use after free in WebRTC
CVE-2023-3727	Chromium: CVE-2023-3727 Use after free in WebRTC
CVE-2023-36887	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-36884	Office and Windows HTML Remote Code Execution Vulnerability
CVE-2023-36874	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2023-36871	Azure Active Directory Security Feature Bypass Vulnerability
CVE-2023-35392	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2023-35367	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2023-35366	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2023-35365	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
CVE-2023-35364	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35363	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35362	Windows Clip Service Elevation of Privilege Vulnerability
CVE-2023-35361	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35360	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35358	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35357	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35356	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35353	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
CVE-2023-35352	Windows Remote Desktop Security Feature Bypass Vulnerability
CVE-2023-35351	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability
CVE-2023-35350	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability
CVE-2023-35348	Active Directory Federation Service Security Feature Bypass Vulnerability
CVE-2023-35347	Microsoft Install Service Elevation of Privilege Vulnerability
CVE-2023-35346	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-35345	Windows DNS Server Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-35344	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-35343	Windows Geolocation Service Remote Code Execution Vulnerability
CVE-2023-35342	Windows Image Acquisition Elevation of Privilege Vulnerability
CVE-2023-35341	Microsoft DirectMusic Information Disclosure Vulnerability
CVE-2023-35340	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2023-35339	Windows CryptoAPI Denial of Service Vulnerability
CVE-2023-35338	Windows Peer Name Resolution Protocol Denial of Service Vulnerability
CVE-2023-35337	Win32k Elevation of Privilege Vulnerability
CVE-2023-35336	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-35332	Windows Remote Desktop Protocol Security Feature Bypass
CVE-2023-35331	Windows Local Security Authority (LSA) Denial of Service Vulnerability
CVE-2023-35330	Windows Extended Negotiation Denial of Service Vulnerability
CVE-2023-35329	Windows Authentication Denial of Service Vulnerability
CVE-2023-35328	Windows Transaction Manager Elevation of Privilege Vulnerability
CVE-2023-35326	Windows CDP User Components Information Disclosure Vulnerability
CVE-2023-35325	Windows Print Spooler Information Disclosure Vulnerability
CVE-2023-35324	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-35323	Windows OLE Remote Code Execution Vulnerability
CVE-2023-35322	Windows Deployment Services Remote Code Execution Vulnerability
CVE-2023-35321	Windows Deployment Services Denial of Service Vulnerability
CVE-2023-35320	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
CVE-2023-35319	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-35318	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-35317	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
CVE-2023-35316	Remote Procedure Call Runtime Information Disclosure Vulnerability
CVE-2023-35315	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
CVE-2023-35314	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-35313	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability
CVE-2023-35312	SYS Elevation of Privilege Vulnerability
CVE-2023-35310	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-35309	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-35308	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-35306	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-35305	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35304	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-35303	USB Audio Class System Driver Remote Code Execution Vulnerability
CVE-2023-35302	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-35300	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-35299	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-35298	sys Denial of Service Vulnerability
CVE-2023-35297	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-35296	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-33174	Windows Cryptographic Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

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

CVE-2023-32030	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
CVE-2023-32022	No Vulnerability Name Found
CVE-2023-32021	Windows SMB Witness Service Security Feature Bypass Vulnerability
CVE-2023-32020	Windows DNS Spoofing Vulnerability
CVE-2023-32019	Windows Kernel Information Disclosure Vulnerability
CVE-2023-32017	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
CVE-2023-32016	Windows Installer Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-32015	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-32014	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-32013	Windows Hyper-V Denial of Service Vulnerability
CVE-2023-32012	Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2023-32011	Windows iSCSI Discovery Service Denial of Service Vulnerability
CVE-2023-32009	Windows Collaborative Translation Framework Elevation of Privilege Vulnerability
CVE-2023-32008	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2023-29373	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2023-29372	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-29371	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-29370	Windows Media Remote Code Execution Vulnerability
CVE-2023-29369	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-29368	Windows Filtering Platform Elevation of Privilege Vulnerability
CVE-2023-29367	iSCSI Target WMI Provider Remote Code Execution Vulnerability
CVE-2023-29366	Windows Geolocation Service Remote Code Execution Vulnerability
CVE-2023-29365	Windows Media Remote Code Execution Vulnerability
CVE-2023-29364	Windows Authentication Elevation of Privilege Vulnerability
CVE-2023-29363	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-29362	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2023-29361	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-29360	Windows TPM Device Driver Elevation of Privilege Vulnerability
CVE-2023-29359	GDI Elevation of Privilege Vulnerability
CVE-2023-29358	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-29355	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-29352	Windows Remote Desktop Security Feature Bypass Vulnerability
CVE-2023-29351	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2023-29346	NTFS Elevation of Privilege Vulnerability
CVE-2023-29336	Win32k Elevation of Privilege Vulnerability
CVE-2023-29331	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-29326	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-29325	Windows OLE Remote Code Execution Vulnerability
CVE-2023-29324	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-28283	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2023-28251	Windows Driver Revocation List Security Feature Bypass Vulnerability
CVE-2023-24949	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-24948	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2023-24947	Windows Bluetooth Driver Remote Code Execution Vulnerability
CVE-2023-24946	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2023-24945	Windows iSCSI Target Service Information Disclosure Vulnerability
CVE-2023-24944	Windows Bluetooth Driver Information Disclosure Vulnerability
CVE-2023-24943	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-24942	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-24941	Windows Network File System Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-24940	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability
CVE-2023-24939	Server for NFS Denial of Service Vulnerability
CVE-2023-24938	Windows CryptoAPI Denial of Service Vulnerability
CVE-2023-24937	Windows CryptoAPI Denial of Service Vulnerability
CVE-2023-24936	Server for NFS Denial of Service Vulnerability
CVE-2023-24932	Secure Boot Security Feature Bypass Vulnerability
CVE-2023-24905	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2023-24903	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2023-24902	Win32k Elevation of Privilege Vulnerability
CVE-2023-24901	Windows NFS Portmapper Information Disclosure Vulnerability
CVE-2023-24900	Windows NTLM Security Support Provider Information Disclosure Vulnerability
CVE-2023-24899	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24898	Windows SMB Denial of Service Vulnerability
CVE-2023-24897	Server for NFS Denial of Service Vulnerability
CVE-2023-24895	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
CVE-2023-33145	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2023-33143	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-3079	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)
CVE-2023-2941	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)
CVE-2023-2940	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)
CVE-2023-2939	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)
CVE-2023-2938	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)
CVE-2023-2937	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)
CVE-2023-2936	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)
CVE-2023-2935	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)
CVE-2023-29345	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
CVE-2023-2934	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)

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

http://buildings.honeywell.com/security

CVE-2023-2933	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)
CVE-2023-2932	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)
CVE-2023-2931	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)
CVE-2023-2930	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)
CVE-2023-2929	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)
CVE-2023-2726	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)
CVE-2023-2725	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)
CVE-2023-2724	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)
CVE-2023-2723	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)
CVE-2023-2722	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)
CVE-2023-2721	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)
CVE-2023-33145	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2023-29336	Win32k Elevation of Privilege Vulnerability
CVE-2023-29325	Windows OLE Remote Code Execution Vulnerability
CVE-2023-29324	Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2023-28308	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28307	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28306	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28305	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28302	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-28298	Windows Kernel Denial of Service Vulnerability
CVE-2023-28297	Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability
CVE-2023-28293	Windows Kernel Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-28283	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2023-28278	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28277	Windows DNS Server Information Disclosure Vulnerability
CVE-2023-28276	Windows Group Policy Security Feature Bypass Vulnerability
CVE-2023-28275	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-28274	Windows Win32k Elevation of Privilege Vulnerability
CVE-2023-28273	Windows Clip Service Elevation of Privilege Vulnerability
CVE-2023-28272	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28271	Windows Kernel Memory Information Disclosure Vulnerability
CVE-2023-28270	Windows Lock Screen Security Feature Bypass Vulnerability
CVE-2023-28269	Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2023-28268	Netlogon RPC Elevation of Privilege Vulnerability
CVE-2023-28267	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2023-28266	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2023-28256	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28255	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28254	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28253	Windows Kernel Information Disclosure Vulnerability
CVE-2023-28252	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-28251	Windows Driver Revocation List Security Feature Bypass Vulnerability
CVE-2023-28250	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-28249	Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2023-28248	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28247	Windows Network File System Information Disclosure Vulnerability
CVE-2023-28246	Windows Registry Elevation of Privilege Vulnerability
CVE-2023-28244	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2023-28243	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-28241	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
CVE-2023-28240	Windows Network Load Balancing Remote Code Execution Vulnerability
CVE-2023-28238	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
CVE-2023-28237	Windows Kernel Remote Code Execution Vulnerability
CVE-2023-28236	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28235	Windows Lock Screen Security Feature Bypass Vulnerability
CVE-2023-28234	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-28233	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-28232	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28231	DHCP Server Service Remote Code Execution Vulnerability
CVE-2023-28229	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2023-28228	Windows Spoofing Vulnerability
CVE-2023-28227	Windows Bluetooth Driver Remote Code Execution Vulnerability
CVE-2023-28226	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2023-28225	Windows NTLM Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
CVE-2023-28224	
CVE-2023-28223	Windows Domain Name Service Remote Code Execution Vulnerability
CVE-2023-28222	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28221	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2023-28220	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28219	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28218	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2023-28217	Windows Network Address Translation (NAT) Denial of Service Vulnerability
CVE-2023-28216	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2023-24949	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-24948	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2023-24947	Windows Bluetooth Driver Remote Code Execution Vulnerability
CVE-2023-24946	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2023-24945	Windows iSCSI Target Service Information Disclosure Vulnerability
CVE-2023-24944	Windows Bluetooth Driver Information Disclosure Vulnerability
CVE-2023-24943	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-24942	Remote Procedure Call Runtime Denial of Service Vulnerability
CVE-2023-24941	Windows Network File System Remote Code Execution Vulnerability
CVE-2023-24940	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability
CVE-2023-24939	Server for NFS Denial of Service Vulnerability
CVE-2023-24932	Secure Boot Security Feature Bypass Vulnerability
CVE-2023-24931	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-24929	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24928	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24927	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24926	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24925	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24924	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24912	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24905	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2023-24903	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2023-24902	Win32k Elevation of Privilege Vulnerability
CVE-2023-24901	Windows NFS Portmapper Information Disclosure Vulnerability
CVE-2023-24900	Windows NTLM Security Support Provider Information Disclosure Vulnerability
CVE-2023-24899	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24898	Windows SMB Denial of Service Vulnerability
CVE-2023-24887	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24886	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24885	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24884	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24883	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-21769	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-21729	Remote Procedure Call Runtime Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-21727	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-21554	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-29354	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
CVE-2023-29350	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-29334	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2023-24935	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2023-2468	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)
CVE-2023-2467	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)
CVE-2023-2466	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)
CVE-2023-2465	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)
CVE-2023-2464	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)
CVE-2023-2463	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)
CVE-2023-2462	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)
CVE-2023-2460	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)
CVE-2023-2459	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)
CVE-2023-2137	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)
CVE-2023-2136	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)
CVE-2023-2135	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)
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)

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

http://buildings.honeywell.com/security

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)
CVE-2023-1810	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)

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

http://buildings.honeywell.com/security

CVE-2023-28308	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28307	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28306	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28305	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28302	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-28298	Windows Kernel Denial of Service Vulnerability
CVE-2023-28297	Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability
CVE-2023-28293	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28278	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28277	Windows DNS Server Information Disclosure Vulnerability
CVE-2023-28276	Windows Group Policy Security Feature Bypass Vulnerability
CVE-2023-28275	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-28274	Windows Win32k Elevation of Privilege Vulnerability
CVE-2023-28273	Windows Clip Service Elevation of Privilege Vulnerability
CVE-2023-28272	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28271	Windows Kernel Memory Information Disclosure Vulnerability
CVE-2023-28270	Windows Lock Screen Security Feature Bypass Vulnerability
CVE-2023-28269	Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2023-28268	Netlogon RPC Elevation of Privilege Vulnerability
CVE-2023-28267	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2023-28266	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2023-28256	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28255	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28254	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-28253	Windows Kernel Information Disclosure Vulnerability
CVE-2023-28252	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-28250	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2023-28249	Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2023-28248	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28247	Windows Network File System Information Disclosure Vulnerability
CVE-2023-28246	Windows Registry Elevation of Privilege Vulnerability
CVE-2023-28244	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2023-28243	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-28241	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
CVE-2023-28240	Windows Network Load Balancing Remote Code Execution Vulnerability
CVE-2023-28238	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
CVE-2023-28237	Windows Kernel Remote Code Execution Vulnerability
CVE-2023-28236	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28235	Windows Lock Screen Security Feature Bypass Vulnerability
CVE-2023-28234	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-28233	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-28232	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28231	DHCP Server Service Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-28229	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2023-28228	Windows Spoofing Vulnerability
CVE-2023-28227	Windows Bluetooth Driver Remote Code Execution Vulnerability
CVE-2023-28226	Windows Enroll Engine Security Feature Bypass Vulnerability
CVE-2023-28225	Windows NTLM Elevation of Privilege Vulnerability
CVE-2023-28224	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
CVE-2023-28223	Windows Domain Name Service Remote Code Execution Vulnerability
CVE-2023-28222	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-28221	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2023-28220	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28219	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-28218	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2023-28217	Windows Network Address Translation (NAT) Denial of Service Vulnerability
CVE-2023-28216	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2023-24931	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-24929	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24928	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24927	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24926	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24925	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24924	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24914	Win32k Elevation of Privilege Vulnerability
CVE-2023-24912	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24887	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24886	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24885	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24884	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24883	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-21769	Microsoft Message Queuing Denial of Service Vulnerability
CVE-2023-21729	Remote Procedure Call Runtime Information Disclosure Vulnerability
CVE-2023-21727	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-21554	Microsoft Message Queuing Remote Code Execution Vulnerability
CVE-2023-24935	Microsoft Edge (Chromium-based) Spoofing Vulnerability
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)

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

http://buildings.honeywell.com/security

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)
CVE-2023-1810	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)
CVE-2023-24913	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24911	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24910	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24909	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24908	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-24907	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24906	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24892	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability
CVE-2023-24880	Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2023-24876	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24872	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24871	Windows Bluetooth Service Remote Code Execution Vulnerability
CVE-2023-24870	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-24869	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-24868	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24867	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-24866	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24865	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24864	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability
CVE-2023-24863	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24862	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-24861	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-24859	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
CVE-2023-24858	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24857	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-24856	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
CVE-2023-23423	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-23422	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-23421	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-23420	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-23417	Windows Partition Management Driver Elevation of Privilege Vulnerability
CVE-2023-23416	Windows Cryptographic Services Remote Code Execution Vulnerability
CVE-2023-23415	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability
CVE-2023-23414	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
CVE-2023-23413	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-23412	Windows Accounts Picture Elevation of Privilege Vulnerability
CVE-2023-23411	Windows Hyper-V Denial of Service Vulnerability
CVE-2023-23410	sys Elevation of Privilege Vulnerability
CVE-2023-23409	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability
CVE-2023-23407	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
CVE-2023-23406	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-23405	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2023-23404	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2023-23403	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
CVE-2023-23402	Windows Media Remote Code Execution Vulnerability
CVE-2023-23401	Windows Media Remote Code Execution Vulnerability
CVE-2023-23400	Windows DNS Server Remote Code Execution Vulnerability
CVE-2023-23394	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability
CVE-2023-23393	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability
CVE-2023-23392	HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2023-23388	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2023-23385	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability
CVE-2023-21708	Remote Procedure Call Runtime Remote Code Execution Vulnerability
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)

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

http://buildings.honeywell.com/security

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)
CVE-2023-1218	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)

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

http://buildings.honeywell.com/security

CVE-2023-1217	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)
CVE-2023-1216	Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convienced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity High)
CVE-2023-1215	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)
CVE-2023-1214	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)
CVE-2023-1213	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)
CVE-2023-1018	0's Module Library allowing a 2-byte read past the end of a TPM2
CVE-2023-1017	0's Module Library allowing writing of a 2-byte data past the end of TPM2
CVE-2023-21808	NET and Visual Studio Remote Code Execution Vulnerability
CVE-2023-21802	Windows Media Remote Code Execution Vulnerability
CVE-2023-21803	Windows iSCSI Discovery Service Remote Code Execution Vulnerability
CVE-2023-21804	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-21805	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2023-21688	NT OS Kernel Elevation of Privilege Vulnerability
CVE-2023-21820	Windows Distributed File System (DFS) Remote Code Execution Vulnerability
CVE-2023-21700	Windows iSCSI Discovery Service Denial of Service Vulnerability
CVE-2023-21689	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21722	NET Framework Denial of Service Vulnerability
CVE-2023-21701	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability
CVE-2023-21822	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2023-21823	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2023-21702	Windows iSCSI Service Denial of Service Vulnerability
CVE-2023-21801	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
CVE-2023-21684	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
CVE-2023-21685	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-21686	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-21691	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability
CVE-2023-21692	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21693	Microsoft PostScript Printer Driver Information Disclosure Vulnerability
CVE-2023-23376	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-21694	Windows Fax Service Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-21690	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21817	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2023-21818	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-21819	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-21813	Windows Secure Channel Denial of Service Vulnerability
CVE-2023-21816	Windows Active Directory Domain Services API Denial of Service Vulnerability
CVE-2023-21699	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
CVE-2023-21798	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2023-21799	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-21811	Windows iSCSI Service Denial of Service Vulnerability
CVE-2023-21812	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-21695	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21697	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
CVE-2023-21797	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2023-0700	Chromium:CVE-2023-0700 Inappropriate implementation in Download
CVE-2023-0701	Chromium:CVE-2023-0701 Heap buffer overflow in WebUI
CVE-2023-0698	Chromium:CVE-2023-0698 Out of bounds read in WebRTC
CVE-2023-0699	Chromium:CVE-2023-0699 Use after free in GPU
CVE-2023-0704	Chromium:CVE-2023-0704 Insufficient policy enforcement in DevTools
CVE-2023-0705	Chromium:CVE-2023-0705 Integer overflow in Core
CVE-2023-0702	Chromium:CVE-2023-0702 Type Confusion in Data Transfer
CVE-2023-0703	Chromium:CVE-2023-0703 Type Confusion in DevTools
CVE-2023-0696	Chromium:CVE-2023-0696 Type Confusion in V8
CVE-2023-21794	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2023-0697	Chromium: CVE-2023-0697 Inappropriate implementation in Full screen mode
CVE-2023-21720	Microsoft Edge (Chromium-based) Tampering Vulnerability
CVE-2023-21687	HTTP.sys Information Disclosure Vulnerability
CVE-2023-21796	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-21795	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2023-21776	Windows Kernel Information Disclosure Vulnerability
CVE-2023-21775	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-21775	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2023-21774	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21773	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21772	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21771	Windows Local Session Manager (LSM) Elevation of Privilege Vulnerability
CVE-2023-21768	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2023-21767	Windows Overlay Filter Elevation of Privilege Vulnerability
CVE-2023-21766	Windows Overlay Filter Information Disclosure Vulnerability
CVE-2023-21765	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2023-21760	Windows Print Spooler Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2023-21759	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability
CVE-2023-21758	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
CVE-2023-21757	Windows Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability
CVE-2023-21755	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21754	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21753	Event Tracing for Windows Information Disclosure Vulnerability
CVE-2023-21752	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2023-21750	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21749	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21748	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21747	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21746	Windows NTLM Elevation of Privilege Vulnerability
CVE-2023-21739	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2023-21733	Windows Bind Filter Driver Elevation of Privilege Vulnerability
CVE-2023-21732	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2023-21730	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2023-21728	Windows Netlogon Denial of Service Vulnerability
CVE-2023-21726	Windows Credential Manager User Interface Elevation of Privilege Vulnerability
CVE-2023-21724	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2023-21719	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
CVE-2023-21683	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
CVE-2023-21682	Windows Point-to-Point Protocol (PPP) Information Disclosure Vulnerability
CVE-2023-21681	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2023-21680	Windows Win32k Elevation of Privilege Vulnerability
CVE-2023-21679	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
CVE-2023-21678	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2023-21677	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
CVE-2023-21676	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2023-21675	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-21674	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2023-21563	BitLocker Security Feature Bypass Vulnerability
CVE-2023-21561	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2023-21560	Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2023-21559	Windows Cryptographic Information Disclosure Vulnerability
CVE-2023-21558	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2023-21557	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
CVE-2023-21556	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
CVE-2023-21555	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
CVE-2023-21552	Windows GDI Elevation of Privilege Vulnerability
CVE-2023-21551	Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2023-21550	Windows Cryptographic Information Disclosure Vulnerability
CVE-2023-21549	Windows SMB Witness Service Elevation of Privilege Vulnerability
CVE-2023-21548	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

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

2022 – Microsoft® Patches Tested with Pro-Watch:

CVE-2022-44708	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-44707	Windows Kernel Denial of Service Vulnerability
CVE-2022-44698	Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2022-44697	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-44689	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability
CVE-2022-44688	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2022-44683	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-44682	Windows Hyper-V Denial of Service Vulnerability
CVE-2022-44681	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-44680	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-44679	Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-44678	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-44677	Windows Projected File System Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-44676	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2022-44675	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2022-44674	Windows Bluetooth Driver Information Disclosure Vulnerability
CVE-2022-44673	Windows Client Server Run-Time Subsystem (CSRSS) Elevation of Privilege Vulnerability
CVE-2022-44671	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-44670	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2022-44669	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2022-44668	Windows Media Remote Code Execution Vulnerability
CVE-2022-44667	Windows Media Remote Code Execution Vulnerability
CVE-2022-44666	Windows Contacts Remote Code Execution Vulnerability
CVE-2022-4440	Chromium: CVE-2022-4440 Use after free in Profiles
CVE-2022-4439	Chromium: CVE-2022-4439 Use after free in Aura
CVE-2022-4438	Chromium: CVE-2022-4438 Use after free in Blink Frames
CVE-2022-4437	Chromium: CVE-2022-4437 Use after free in Mojo IPC
CVE-2022-4436	Chromium: CVE-2022-4436 Use after free in Blink Media
CVE-2022-4195	Chromium: CVE-2022-4195 Insufficient policy enforcement in Safe Browsing
CVE-2022-4194	Chromium: CVE-2022-4194 Use after free in Accessibility
CVE-2022-4193	Chromium: CVE-2022-4193 Insufficient policy enforcement in File System API
CVE-2022-4192	Chromium: CVE-2022-4192 Use after free in Live Caption
CVE-2022-4191	Chromium: CVE-2022-4191 Use after free in Sign-In
CVE-2022-4190	Chromium: CVE-2022-4190 Insufficient data validation in Directory
CVE-2022-4189	Chromium: CVE-2022-4189 Insufficient policy enforcement in DevTools
CVE-2022-4188	Chromium: CVE-2022-4188 Insufficient validation of untrusted input in CORS
CVE-2022-4187	Chromium: CVE-2022-4187 Insufficient policy enforcement in DevTools
CVE-2022-4186	Chromium: CVE-2022-4186 Insufficient validation of untrusted input in Downloads
CVE-2022-4185	Chromium: CVE-2022-4185 Inappropriate implementation in Navigation
CVE-2022-4184	Chromium: CVE-2022-4184 Insufficient policy enforcement in Autofill
CVE-2022-4183	Chromium: CVE-2022-4183 Insufficient policy enforcement in Popup Blocker
CVE-2022-4182	Chromium: CVE-2022-4182 Inappropriate implementation in Fenced Frames
CVE-2022-4181	Chromium: CVE-2022-4181 Use after free in Forms
CVE-2022-4180	Chromium: CVE-2022-4180 Use after free in Mojo
CVE-2022-4179	Chromium: CVE-2022-4179 Use after free in Audio
CVE-2022-4178	Chromium: CVE-2022-4178 Use after free in Mojo
CVE-2022-4177	Chromium: CVE-2022-4177 Use after free in Extensions
CVE-2022-4175	Chromium: CVE-2022-4175 Use after free in Camera Capture
CVE-2022-4174	Chromium: CVE-2022-4174 Type Confusion in V8
CVE-2022-41121	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-41115	Microsoft Edge (Chromium-based) Update Elevation of Privilege Vulnerability
CVE-2022-41094	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2022-41089	.NET Framework Remote Code Execution Vulnerability
CVE-2022-41077	Windows Fax Compose Form Elevation of Privilege Vulnerability
CVE-2022-41076	PowerShell Remote Code Execution Vulnerability
CVE-2022-41074	Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-37967	Windows Kerberos Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

ADV220005	Guidance on Microsoft Signed Drivers Being Used Maliciously
CVE-2022-41128	Windows Scripting Languages Remote Code Execution Vulnerability
CVE-2022-41125	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2022-41118	Windows Scripting Languages Remote Code Execution Vulnerability
CVE-2022-41114	Windows Bind Filter Driver Elevation of Privilege Vulnerability
CVE-2022-41113	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2022-41109	Windows Win32k Elevation of Privilege Vulnerability
CVE-2022-41102	Windows Overlay Filter Elevation of Privilege Vulnerability
CVE-2022-41101	Windows Overlay Filter Elevation of Privilege Vulnerability
CVE-2022-41100	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2022-41099	BitLocker Security Feature Bypass Vulnerability
CVE-2022-41098	Windows GDI+ Information Disclosure Vulnerability
CVE-2022-41097	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability
CVE-2022-41096	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-41095	Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2022-41093	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2022-41092	Windows Win32k Elevation of Privilege Vulnerability
CVE-2022-41091	Windows Mark of the Web Security Feature Bypass Vulnerability
CVE-2022-41090	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
CVE-2022-41088	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-41086	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2022-41073	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-41064	.NET Framework Information Disclosure Vulnerability
CVE-2022-41058	Windows Network Address Translation (NAT) Denial of Service Vulnerability
CVE-2022-41057	Windows HTTP.sys Elevation of Privilege Vulnerability
CVE-2022-41056	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability
CVE-2022-41055	Windows Human Interface Device Information Disclosure Vulnerability
CVE-2022-41054	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
CVE-2022-41053	Windows Kerberos Denial of Service Vulnerability
CVE-2022-41052	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2022-41050	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability
CVE-2022-41049	Windows Mark of the Web Security Feature Bypass Vulnerability
CVE-2022-41048	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2022-41047	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2022-41045	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
CVE-2022-41039	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-3890	Chromium: CVE-2022-3890 Heap buffer overflow in Crashpad
CVE-2022-3889	Chromium: CVE-2022-3889 Type Confusion in V8
CVE-2022-3888	CVE-2022-3888 Use after free in WebCodecs
CVE-2022-3887	CVE-2022-3887 Use after free in Web Workers
CVE-2022-3886	CVE-2022-3886 Use after free in Speech Recognition
CVE-2022-3885	CVE-2022-3885 Use after free in V8
CVE-2022-38023	Netlogon RPC Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-38015	Windows Hyper-V Denial of Service Vulnerability
CVE-2022-37992	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2022-37967	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-37966	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability
CVE-2022-23824	AMD: CVE-2022-23824 IBPB and Return Address Predictor Interactions

CVE-2022-41081	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-41033	Windows COM+ Event System Service Elevation of Privilege Vulnerability
CVE-2022-38051	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-38050	Win32k Elevation of Privilege Vulnerability
CVE-2022-38047	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-38046	Web Account Manager Information Disclosure Vulnerability
CVE-2022-38045	Windows Server Service Elevation of Privilege Vulnerability
CVE-2022-38044	Windows CD-ROM File System Driver Remote Code Execution Vulnerability
CVE-2022-38043	Windows Security Support Provider Interface Information Disclosure Vulnerability
CVE-2022-38042	Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2022-38041	Windows Secure Channel Denial of Service Vulnerability
CVE-2022-38040	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2022-38039	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-38038	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-38037	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-38034	Windows Workstation Service Elevation of Privilege Vulnerability
CVE-2022-38033	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability
CVE-2022-38032	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability
CVE-2022-38031	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2022-38030	Windows USB Serial Driver Information Disclosure Vulnerability
CVE-2022-38029	Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-38028	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-38027	Windows Storage Elevation of Privilege Vulnerability
CVE-2022-38026	Windows DHCP Client Information Disclosure Vulnerability
CVE-2022-38022	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-38021	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
CVE-2022-38016	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
CVE-2022-38003	Windows Resilient File System Elevation of Privilege
CVE-2022-38000	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-37999	Windows Group Policy Preference Client Elevation of Privilege Vulnerability
CVE-2022-37998	Windows Local Session Manager (LSM) Denial of Service Vulnerability
CVE-2022-37997	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-37996	Windows Kernel Memory Information Disclosure Vulnerability
CVE-2022-37995	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-37994	Windows Group Policy Preference Client Elevation of Privilege Vulnerability
CVE-2022-37993	Windows Group Policy Preference Client Elevation of Privilege Vulnerability
CVE-2022-37991	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-37990	Windows Kernel Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-37989	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
CVE-2022-37988	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-37987	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability
CVE-2022-37986	Windows Win32k Elevation of Privilege Vulnerability
CVE-2022-37985	Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-37984	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-37984	Windows WLAN Service Elevation of Privilege Vulnerability
CVE-2022-37983	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-37982	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
CVE-2022-37981	Windows Event Logging Service Denial of Service Vulnerability
CVE-2022-37980	Windows DHCP Client Elevation of Privilege Vulnerability
CVE-2022-37979	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2022-37978	Windows Active Directory Certificate Services Security Feature Bypass
CVE-2022-37977	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability
CVE-2022-37976	Active Directory Certificate Services Elevation of Privilege Vulnerability
CVE-2022-37975	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2022-37974	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability
CVE-2022-37973	Windows Local Session Manager (LSM) Denial of Service Vulnerability
CVE-2022-37970	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-37965	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
CVE-2022-35770	Windows NTLM Spoofing Vulnerability
CVE-2022-33645	Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2022-33635	Windows GDI+ Remote Code Execution Vulnerability
CVE-2022-33634	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-30198	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-24504	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-22035	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability

CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2022-41040	Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2022-41035	Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2022-38006	Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-38005	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-38004	Windows Fax Service Remote Code Execution Vulnerability
CVE-2022-37972	Microsoft Endpoint Configuration Manager Spoofing Vulnerability
CVE-2022-37959	Network Device Enrollment Service (NDES) Security Feature Bypass Vulnerability
CVE-2022-37958	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Information Disclosure Vulnerability
CVE-2022-37957	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-37956	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-37955	Windows Group Policy Elevation of Privilege Vulnerability
CVE-2022-35803	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-3373	Chromium: CVE-2022-3373 Out of bounds write in V8
CVE-2022-3370	Chromium: CVE-2022-3370 Use after free in Custom Elements

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

http://buildings.honeywell.com/security

CVE-2022-3317	Chromium: CVE-2022-3317 Insufficient validation of untrusted input in Intents
CVE-2022-3316	Chromium: CVE-2022-3316 Insufficient validation of untrusted input in Safe Browsing
CVE-2022-3315	Chromium: CVE-2022-3315 Type confusion in Blink
CVE-2022-3313	Chromium: CVE-2022-3313 Incorrect security UI in Full Screen
CVE-2022-3311	Chromium: CVE-2022-3311 Use after free in Import
CVE-2022-3310	Chromium: CVE-2022-3310 Insufficient policy enforcement in Custom Tabs
CVE-2022-3308	Chromium: CVE-2022-3308 Insufficient policy enforcement in Developer Tools
CVE-2022-3307	Chromium: CVE-2022-3307 Use after free in Media
CVE-2022-3304	Chromium: CVE-2022-3304 Use after free in CSS
CVE-2022-3200	Chromium: CVE-2022-3200 Heap buffer overflow in Internals
CVE-2022-3199	Chromium: CVE-2022-3199 Use after free in Frames
CVE-2022-3198	Chromium: CVE-2022-3198 Use after free in PDF
CVE-2022-3197	Chromium: CVE-2022-3197 Use after free in PDF
CVE-2022-3196	Chromium: CVE-2022-3196 Use after free in PDF
CVE-2022-3195	Chromium: CVE-2022-3195 Out of bounds write in Storage
CVE-2022-26929	.NET Framework Remote Code Execution Vulnerability
CVE-2022-35820	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2022-35798	Azure Arc Jumpstart Information Disclosure Vulnerability
CVE-2022-35797	Windows Hello Security Feature Bypass Vulnerability
CVE-2022-35795	Windows Error Reporting Service Elevation of Privilege Vulnerability
CVE-2022-35794	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2022-35793	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-35792	Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-35771	Windows Defender Credential Guard Elevation of Privilege Vulnerability
CVE-2022-35769	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability
CVE-2022-35768	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-35767	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2022-35766	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
CVE-2022-35765	Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-35764	Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-35763	Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-35760	Microsoft ATA Port Driver Elevation of Privilege Vulnerability
CVE-2022-35754	Unified Write Filter Elevation of Privilege Vulnerability
CVE-2022-34703	Windows Partition Management Driver Elevation of Privilege Vulnerability
CVE-2022-34303	CERT/CC: CVE-20220-34303 Crypto Pro Boot Loader Bypass
CVE-2022-33680	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-33672	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33671	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33670	Windows Partition Management Driver Elevation of Privilege Vulnerability
CVE-2022-33669	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33668	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33667	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33666	Azure Site Recovery Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-33665	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33664	Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33639	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-33638	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-32230	Windows SMB Denial of Service Vulnerability
CVE-2022-30193	AV1 Video Extension Remote Code Execution Vulnerability
CVE-2022-30192	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-30188	HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-30184	.NET and Visual Studio Information Disclosure Vulnerability
CVE-2022-30180	Azure RTOS GUIX Studio Information Disclosure Vulnerability
CVE-2022-30179	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30177	Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30166	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2022-30165	Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-30164	Kerberos AppContainer Security Feature Bypass Vulnerability
CVE-2022-30163	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-30162	Windows Kernel Information Disclosure Vulnerability
CVE-2022-30161	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30160	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
CVE-2022-30155	Windows Kernel Denial of Service Vulnerability
CVE-2022-30154	Microsoft File Server Shadow Copy Agent Service (RVSS) Elevation of Privilege Vulnerability
CVE-2022-30153	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30138	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-30130	.NET Framework Denial of Service Vulnerability
CVE-2022-29149	Azure Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability
CVE-2022-29143	Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2022-29142	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-29141	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29140	Windows Print Spooler Information Disclosure Vulnerability
CVE-2022-29139	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29138	Windows Clustered Shared Volume Elevation of Privilege Vulnerability
CVE-2022-29137	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29135	Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
CVE-2022-29134	Windows Clustered Shared Volume Information Disclosure Vulnerability
CVE-2022-29132	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-29131	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29130	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29129	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29128	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-27776	HackerOne: CVE-2022-27776 Insufficiently protected credentials vulnerability might leak authentication or cookie header data
CVE-2022-26920	Windows Graphics Component Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-26919	Windows LDAP Remote Code Execution Vulnerability
CVE-2022-26918	Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26917	Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26916	Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26915	Windows Secure Channel Denial of Service Vulnerability
CVE-2022-26904	Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2022-26832	.NET Framework Denial of Service Vulnerability
CVE-2022-26831	Windows LDAP Denial of Service Vulnerability
CVE-2022-26828	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2022-26827	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2022-26825	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26824	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26823	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26822	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26821	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26812	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26811	Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26810	Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2022-26809	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-26808	Windows File Explorer Elevation of Privilege Vulnerability
CVE-2022-26807	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2022-26803	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26802	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26801	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26798	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26797	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26796	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26794	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26792	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26790	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26789	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26787	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26786	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-24525	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2022-24512	.NET and Visual Studio Remote Code Execution Vulnerability
CVE-2022-24507	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2022-24503	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2022-24502	Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2022-24464	.NET and Visual Studio Denial of Service Vulnerability
CVE-2022-24460	Tablet Windows User Interface Application Elevation of Privilege Vulnerability
CVE-2022-24459	Windows Fax and Scan Service Elevation of Privilege Vulnerability
CVE-2022-24455	Windows CD-ROM Driver Elevation of Privilege Vulnerability
CVE-2022-24454	Windows Security Support Provider Interface Elevation of Privilege Vulnerability
CVE-2022-23825	AMD: CVE-2022-23825 AMD CPU Branch Type Confusion

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

http://buildings.honeywell.com/security

CVE-2022-23299	Windows PDEV Elevation of Privilege Vulnerability
CVE-2022-23298	Windows NT OS Kernel Elevation of Privilege Vulnerability
CVE-2022-23297	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
CVE-2022-23296	Windows Installer Elevation of Privilege Vulnerability
CVE-2022-23294	Windows Event Tracing Remote Code Execution Vulnerability
CVE-2022-23293	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
CVE-2022-23291	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-23290	Windows Inking COM Elevation of Privilege Vulnerability
CVE-2022-23288	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-23287	Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-23285	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-23284	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-23283	Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-23281	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2022-23278	Microsoft Defender for Endpoint Spoofing Vulnerability
CVE-2022-23253	Point-to-Point Tunneling Protocol Denial of Service Vulnerability
CVE-2022-22050	Windows Fax Service Elevation of Privilege Vulnerability
CVE-2022-22049	Windows CSRSS Elevation of Privilege Vulnerability
CVE-2022-22048	BitLocker Security Feature Bypass Vulnerability
CVE-2022-22047	Windows CSRSS Elevation of Privilege Vulnerability
CVE-2022-22045	Windows.Devices.Picker.dll Elevation of Privilege Vulnerability
CVE-2022-22043	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
CVE-2022-22042	Windows Hyper-V Information Disclosure Vulnerability
CVE-2022-22041	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22040	Internet Information Services Dynamic Compression Module Denial of Service Vulnerability
CVE-2022-22039	Windows Network File System Remote Code Execution Vulnerability
CVE-2022-22019	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-22010	Media Foundation Information Disclosure Vulnerability
CVE-2022-22002	Windows User Account Profile Picture Denial of Service Vulnerability
CVE-2022-22001	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-22000	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21999	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-21998	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2022-21997	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-21995	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-21994	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-21993	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2022-21992	Windows Mobile Device Management Remote Code Execution Vulnerability
CVE-2022-21989	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-21981	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21977	Media Foundation Information Disclosure Vulnerability
CVE-2022-21963	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21962	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21961	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2022-21960	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21959	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21958	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21928	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21924	Workstation Service Remote Protocol Security Feature Bypass Vulnerability
CVE-2022-21913	Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass
CVE-2022-21911	.NET Framework Denial of Service Vulnerability
CVE-2022-21908	Windows Installer Elevation of Privilege Vulnerability
CVE-2022-21907	HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2022-21906	Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2022-21905	Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2022-21904	Windows GDI Information Disclosure Vulnerability
CVE-2022-21903	Windows GDI Elevation of Privilege Vulnerability
CVE-2022-21902	Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-21901	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2022-21900	Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2022-21899	Windows Extensible Firmware Interface Security Feature Bypass Vulnerability
CVE-2022-21898	DirectX Graphics Kernel Remote Code Execution Vulnerability
CVE-2022-21897	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21894	Secure Boot Security Feature Bypass Vulnerability
CVE-2022-21890	Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21889	Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21888	Windows Modern Execution Server Remote Code Execution Vulnerability
CVE-2022-21885	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-21884	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2022-21883	Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21882	Win32k Elevation of Privilege Vulnerability
CVE-2022-21881	Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-21880	Windows GDI+ Information Disclosure Vulnerability
CVE-2022-21874	Windows Security Center API Remote Code Execution Vulnerability
CVE-2022-21843	Windows IKE Extension Denial of Service Vulnerability
CVE-2022-2481	Chromium: CVE-2022-2481 Use after free in Views
CVE-2022-2480	Chromium: CVE-2022-2480 Use after free in Service Worker API
CVE-2022-2479	Chromium: CVE-2022-2479 Insufficient validation of untrusted input in File
CVE-2022-2478	Chromium: CVE-2022-2478 Use after free in PDF
CVE-2022-2477	Chromium: CVE-2022-2477 Use after free in Guest View
CVE-2022-2295	Chromium: CVE-2022-2295 Type Confusion in V8
CVE-2022-2294	Chromium: CVE-2022-2294 Heap buffer overflow in WebRTC
CVE-2022-2165	Chromium: CVE-2022-2165 Insufficient data validation in URL formatting
CVE-2022-2164	Chromium: CVE-2022-2164 Inappropriate implementation in Extensions API
CVE-2022-2163	Chromium: CVE-2022-2163 Use after free in Cast UI and Toolbar
CVE-2022-2162	Chromium: CVE-2022-2162 Insufficient policy enforcement in File System API
CVE-2022-2161	Chromium: CVE-2022-2161 Use after free in WebApp Provider
CVE-2022-2160	Chromium: CVE-2022-2160 Insufficient policy enforcement in DevTools

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

http://buildings.honeywell.com/security

CVE-2022-2158	Chromium: CVE-2022-2158 Type Confusion in V8
CVE-2022-2157	Chromium: CVE-2022-2157 Use after free in Interest groups
CVE-2022-2156	Chromium: CVE-2022-2156 Use after free in Base

2021 – Microsoft® Patches Tested with Pro-Watch

CVE-2021-43893	Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability
CVE-2021-43883	Windows Installer Elevation of Privilege Vulnerability
CVE-2021-43877	ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability
CVE-2021-43248	Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2021-43247	Windows TCP/IP Driver Elevation of Privilege Vulnerability
CVE-2021-43246	Windows Hyper-V Denial of Service Vulnerability
CVE-2021-43245	Windows Digital TV Tuner Elevation of Privilege Vulnerability
CVE-2021-43244	Windows Kernel Information Disclosure Vulnerability
CVE-2021-43240	NTFS Set Short Name Elevation of Privilege Vulnerability
CVE-2021-43239	Windows Recovery Environment Agent Elevation of Privilege Vulnerability
CVE-2021-43238	Windows Remote Access Elevation of Privilege Vulnerability
CVE-2021-43237	Windows Setup Elevation of Privilege Vulnerability
CVE-2021-43236	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2021-43235	Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-43234	Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-43233	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2021-43232	Windows Event Tracing Remote Code Execution Vulnerability
CVE-2021-43231	Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43230	Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43229	Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43228	SymCrypt Denial of Service Vulnerability
CVE-2021-43227	Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-43226	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-43224	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2021-43223	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-43222	Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2021-43219	DirectX Graphics Kernel File Denial of Service Vulnerability
CVE-2021-43217	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
CVE-2021-43216	Microsoft Local Security Authority Server (lsasrv) Information Disclosure Vulnerability
CVE-2021-43215	iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution
CVE-2021-43207	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-42291	Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42288	Windows Hello Security Feature Bypass Vulnerability
CVE-2021-42287	Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42285	Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-42284	Windows Hyper-V Denial of Service Vulnerability
CVE-2021-42283	NTFS Elevation of Privilege Vulnerability
CVE-2021-42282	Active Directory Domain Services Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-42279	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2021-42278	Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42275	Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2021-41367	NTFS Elevation of Privilege Vulnerability
CVE-2021-41361	Active Directory Federation Server Spoofing Vulnerability
CVE-2021-41357	Win32k Elevation of Privilege Vulnerability
CVE-2021-41351	Microsoft Edge (Chrome based) Spoofing on IE Mode
CVE-2021-41347	Windows AppX Deployment Service Elevation of Privilege Vulnerability
CVE-2021-41346	Console Window Host Security Feature Bypass Vulnerability
CVE-2021-41345	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-41343	Windows Fast FAT File System Driver Information Disclosure Vulnerability
CVE-2021-41342	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-41340	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-41339	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2021-41338	Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability
CVE-2021-41337	Active Directory Security Feature Bypass Vulnerability
CVE-2021-41335	Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-41334	Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2021-41333	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-41332	Windows Print Spooler Information Disclosure Vulnerability
CVE-2021-41331	Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2021-41330	Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-40489	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-40488	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-40478	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-40477	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-40476	Windows AppContainer Elevation Of Privilege Vulnerability
CVE-2021-40475	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
CVE-2021-40470	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2021-40469	Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-40468	Windows Bind Filter Driver Information Disclosure Vulnerability
CVE-2021-40467	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40466	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40465	Windows Text Shaping Remote Code Execution Vulnerability
CVE-2021-40464	Windows Nearby Sharing Elevation of Privilege Vulnerability
CVE-2021-40463	Windows NAT Denial of Service Vulnerability
CVE-2021-40462	Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability
CVE-2021-40461	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2021-40460	Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability
CVE-2021-40456	Windows AD FS Security Feature Bypass Vulnerability
CVE-2021-40455	Windows Installer Spoofing Vulnerability
CVE-2021-40454	Rich Text Edit Control Information Disclosure Vulnerability
CVE-2021-40450	Win32k Elevation of Privilege Vulnerability
CVE-2021-40449	Win32k Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-40447	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-40443	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40441	Windows Media Center Elevation of Privilege Vulnerability
CVE-2021-38671	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-38667	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-38663	Windows exFAT File System Information Disclosure Vulnerability
CVE-2021-38662	Windows Fast FAT File System Driver Information Disclosure Vulnerability
CVE-2021-38639	Win32k Elevation of Privilege Vulnerability
CVE-2021-38638	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2021-38637	Windows Storage Information Disclosure Vulnerability
CVE-2021-38624	Windows Key Storage Provider Security Feature Bypass Vulnerability
CVE-2021-36970	Windows Print Spooler Spoofing Vulnerability
CVE-2021-36967	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
CVE-2021-36965	Windows WLAN AutoConfig Service Remote Code Execution Vulnerability
CVE-2021-36953	Windows TCP/IP Denial of Service Vulnerability
CVE-2021-36948	Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2021-36938	Windows Cryptographic Primitives Library Information Disclosure Vulnerability
CVE-2021-36937	Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability
CVE-2021-36936	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-36933	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36932	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36927	Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability
CVE-2021-36926	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-34456	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-34447	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-34500	Windows Kernel Memory Information Disclosure Vulnerability
CVE-2021-34514	Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-34511	Windows Installer Elevation of Privilege Vulnerability
CVE-2021-34446	Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2021-34496	Windows GDI Information Disclosure Vulnerability
CVE-2021-34498	Windows GDI Elevation of Privilege Vulnerability
CVE-2021-34455	Windows File History Service Elevation of Privilege Vulnerability
CVE-2021-34494	Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-34444	Windows DNS Server Denial of Service Vulnerability
CVE-2021-34461	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2021-34492	Windows Certificate Spoofing Vulnerability
CVE-2021-34459	Windows AppContainer Elevation Of Privilege Vulnerability
CVE-2021-34504	Windows Address Book Remote Code Execution Vulnerability
CVE-2021-34516	Win32k Elevation of Privilege Vulnerability
CVE-2021-34509	Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-34513	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34512	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34448	Scripting Engine Memory Corruption Vulnerability
CVE-2021-34476	Bowser.sys Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-33739	Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2021-31977	Windows Hyper-V Denial of Service Vulnerability
CVE-2021-31976	Server for NFS Information Disclosure Vulnerability
CVE-2021-31975	Server for NFS Information Disclosure Vulnerability
CVE-2021-31974	Server for NFS Denial of Service Vulnerability
CVE-2021-31973	Windows GPSVC Elevation of Privilege Vulnerability
CVE-2021-31972	Event Tracing for Windows Information Disclosure Vulnerability
CVE-2021-31971	Windows HTML Platform Security Feature Bypass Vulnerability
CVE-2021-31970	Windows TCP/IP Driver Security Feature Bypass Vulnerability
CVE-2021-31959	Scripting Engine Memory Corruption Vulnerability
CVE-2021-31194	OLE Automation Remote Code Execution Vulnerability
CVE-2021-31193	Windows SSDP Service Elevation of Privilege Vulnerability
CVE-2021-31191	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-31190	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2021-31188	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2021-31187	Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-31186	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2021-28447	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
CVE-2021-28446	Windows Portmapping Information Disclosure Vulnerability
CVE-2021-28445	Windows Network File System Remote Code Execution Vulnerability
CVE-2021-28444	Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2021-28443	Windows Console Driver Denial of Service Vulnerability
CVE-2021-28442	Windows TCP/IP Information Disclosure Vulnerability
CVE-2021-28441	Windows Hyper-V Information Disclosure Vulnerability
CVE-2021-28440	Windows Installer Elevation of Privilege Vulnerability
CVE-2021-28439	Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-28438	Windows Console Driver Denial of Service Vulnerability
CVE-2021-28437	Windows Installer Information Disclosure Vulnerability
CVE-2021-28436	Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28435	Windows Event Tracing Information Disclosure Vulnerability
CVE-2021-28434	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28358	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28357	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28356	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28355	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28354	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28353	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28352	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28351	Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28350	Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28349	Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28348	Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28347	Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28346	Remote Procedure Call Runtime Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-28345	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28344	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28343	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28342	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28341	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28340	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28339	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28338	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28337	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28336	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28335	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28334	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28333	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28332	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28331	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28330	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28329	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28328	Windows DNS Information Disclosure Vulnerability
CVE-2021-28327	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28326	Windows AppX Deployment Server Denial of Service Vulnerability
CVE-2021-28325	Windows SMB Information Disclosure Vulnerability
CVE-2021-28324	Windows SMB Information Disclosure Vulnerability
CVE-2021-28323	Windows SMB Information Disclosure Vulnerability
CVE-2021-28322	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28321	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28320	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability
CVE-2021-28319	Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-28318	Windows GDI+ Information Disclosure Vulnerability
CVE-2021-28317	Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2021-28316	Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2021-28315	Windows Media Video Decoder Remote Code Execution Vulnerability
CVE-2021-28314	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2021-28313	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28312	Windows NTFS Denial of Service Vulnerability
CVE-2021-28311	Windows Application Compatibility Cache Denial of Service Vulnerability
CVE-2021-28310	Win32k Elevation of Privilege Vulnerability
CVE-2021-28309	Windows Kernel Information Disclosure Vulnerability
CVE-2021-27096	NTFS Elevation of Privilege Vulnerability
CVE-2021-27095	Windows Media Video Decoder Remote Code Execution Vulnerability
CVE-2021-27094	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
CVE-2021-27093	Windows Kernel Information Disclosure Vulnerability
CVE-2021-27092	Azure AD Web Sign-in Security Feature Bypass Vulnerability
CVE-2021-27090	Windows Secure Kernel Mode Elevation of Privilege Vulnerability
CVE-2021-27089	Microsoft Internet Messaging API Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-27088	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-27086	Windows Services and Controller App Elevation of Privilege Vulnerability
CVE-2021-27079	Windows Media Photo Codec Information Disclosure Vulnerability
CVE-2021-27072	Win32k Elevation of Privilege Vulnerability
CVE-2021-26442	Windows HTTP.sys Elevation of Privilege Vulnerability
CVE-2021-26441	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-26435	Windows Scripting Engine Memory Corruption Vulnerability
CVE-2021-26433	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-26432	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability
CVE-2021-26426	Windows User Account Profile Picture Elevation of Privilege Vulnerability
CVE-2021-26424	Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-26419	Scripting Engine Memory Corruption Vulnerability
CVE-2021-26417	Windows Overlay Filter Information Disclosure Vulnerability
CVE-2021-26416	Windows Hyper-V Denial of Service Vulnerability
CVE-2021-26415	Windows Installer Elevation of Privilege Vulnerability
CVE 2021 26414	Windows DCOM Server Security Feature Bypass
CVE-2021-26413	Windows Installer Spoofing Vulnerability
CVE-2021-24111	.NET Framework Denial of Service Vulnerability
CVE-2021-24103	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-24102	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-24098	Windows Console Driver Denial of Service Vulnerability
CVE-2021-24086	Windows TCP/IP Denial of Service Vulnerability
CVE-2021-24082	Microsoft.PowerShell.Utility Module WDAC Security Feature Bypass Vulnerability
CVE-2021-24081	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2021-24076	Microsoft Windows VMSwitch Information Disclosure Vulnerability
CVE-2021-24075	Windows Network File System Denial of Service Vulnerability
CVE-2021-24106	Windows DirectX Information Disclosure Vulnerability
CVE-2021-24096	Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-24094	Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-24093	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-24091	Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2021-24088	Windows Local Spooler Remote Code Execution Vulnerability
CVE-2021-25195	Windows PKU2U Elevation of Privilege Vulnerability
CVE-2021-24084	Windows Mobile Device Management Information Disclosure Vulnerability
CVE-2021-24083	Windows Address Book Remote Code Execution Vulnerability
CVE-2021-24080	Windows Trust Verification API Denial of Service Vulnerability
CVE-2021-24079	Windows Backup Engine Information Disclosure Vulnerability
CVE-2021-24078	Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-24077	Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-24074	Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-1734	Windows Remote Procedure Call Information Disclosure Vulnerability
CVE-2021-1732	Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1731	PFX Encryption Security Feature Bypass Vulnerability
CVE-2021-1727	Windows Installer Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2021-1722	Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-1710	Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-1709	Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1708	Windows GDI+ Information Disclosure Vulnerability
CVE-2021-1706	Windows LUAFV Elevation of Privilege Vulnerability
CVE-2021-1705	Microsoft Edge (HTML-based) Memory Corruption Vulnerability
CVE-2021-1704	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2021-1703	Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2021-1702	Windows Remote Procedure Call Runtime Elevation of Privilege Vulnerability
CVE-2021-1701	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1700	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1699	Windows (modem.sys) Information Disclosure Vulnerability
CVE-2021-1698	Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1697	Windows InstallService Elevation of Privilege Vulnerability
CVE-2021-1696	Windows Graphics Component Information Disclosure Vulnerability
CVE-2021-1695	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-1694	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2021-1693	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1692	Hyper-V Denial of Service Vulnerability
CVE-2021-1691	Hyper-V Denial of Service Vulnerability
CVE-2021-1690	Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1689	Windows Multipoint Management Elevation of Privilege Vulnerability
CVE-2021-1688	Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1687	Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1686	Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1685	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2021-1684	Windows Bluetooth Security Feature Bypass Vulnerability
CVE-2021-1683	Windows Bluetooth Security Feature Bypass Vulnerability
CVE-2021-1682	Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-1681	Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1680	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2021-1679	Windows CryptoAPI Denial of Service Vulnerability
CVE-2021-1678	NTLM Security Feature Bypass Vulnerability
CVE-2021-1676	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
CVE-2021-1674	Windows Remote Desktop Protocol Core Security Feature Bypass Vulnerability
CVE-2021-1673	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1672	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-1671	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1670	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-1669	Windows Remote Desktop Security Feature Bypass Vulnerability
CVE-2021-1668	Microsoft DTV-DVD Video Decoder Remote Code Execution Vulnerability
CVE-2021-1667	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1666	Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1665	GDI+ Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

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

2020 – Microsoft® Patches Tested with Pro-Watch

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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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 dnsrslvr.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
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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
CVE-2020-1306	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1305	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1304	Windows Runtime Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
CVE-2020-1136	Media Foundation Memory Corruption Vulnerability
CVE-2020-1135	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1134	Windows State Repository Service Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2020-1133	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1132	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-1131	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1130	Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1129	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-1126	Media Foundation Memory Corruption Vulnerability
CVE-2020-1125	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1124	Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1123	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1122	Windows Language Pack Installer Elevation of Privilege Vulnerability
CVE-2020-1121	Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1119	Windows Information Disclosure Vulnerability
CVE-2020-1118	Microsoft Windows Transport Layer Security Denial of Service Vulnerability
CVE-2020-1117	Microsoft Color Management Remote Code Execution Vulnerability
CVE-2020-1116	Windows CSRSS Information Disclosure Vulnerability
CVE-2020-1115	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-1114	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1113	Windows Task Scheduler Security Feature Bypass Vulnerability
CVE-2020-1112	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
CVE-2020-1111	Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1110	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-1109	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-1108	.NET Core & .NET Framework Denial of Service Vulnerability
CVE-2020-1098	Windows Shell Infrastructure Component Elevation of Privilege Vulnerability
CVE-2020-1097	Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-1096	Microsoft Edge PDF Remote Code Execution Vulnerability
CVE-2020-1094	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-1093	VBScript Remote Code Execution Vulnerability
CVE-2020-1092	Internet Explorer Memory Corruption Vulnerability
CVE-2020-1091	Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-1090	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1088	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1087	Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1086	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1085	Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-1084	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1083	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1082	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1081	Windows Printer Service Elevation of Privilege Vulnerability
CVE-2020-1080	Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-1079	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-1078	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1077	Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1076	Windows Denial of Service Vulnerability
CVE-2020-1075	Windows Subsystem for Linux Information Disclosure Vulnerability
CVE-2020-1074	Jet Database Engine Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

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
CVE-2020-0949	Media Foundation Memory Corruption Vulnerability
CVE-2020-0948	Media Foundation Memory Corruption Vulnerability
CVE-2020-0947	Media Foundation Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

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
CVE-2020-0878	Microsoft Browser Memory Corruption Vulnerability
CVE-2020-0877	Win32k Elevation of Privilege Vulnerability
CVE-2020-0876	Win32k Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2020-0875	Microsoft splwow64 Information Disclosure Vulnerability
CVE-2020-0874	Windows GDI Information Disclosure Vulnerability
CVE-2020-0871	Windows Network Connections Service Information Disclosure Vulnerability
CVE-2020-0870	Shell infrastructure component Elevation of Privilege Vulnerability
CVE-2020-0869	Media Foundation Memory Corruption Vulnerability
CVE-2020-0868	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-0867	Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-0866	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0865	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0864	Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0863	Connected User Experiences and Telemetry Service Information Disclosure Vulnerability
CVE-2020-0861	Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability
CVE-2020-0860	Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0859	Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2020-0858	Windows Elevation of Privilege Vulnerability
CVE-2020-0857	Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0856	Active Directory Information Disclosure Vulnerability
CVE-2020-0854	Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-0853	CVE-2020-0853 | Windows Imaging Component Information Disclosure Vulnerability
CVE-2020-0849	CVE-2020-0849 | Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0848	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0847	VBScript Remote Code Execution Vulnerability
CVE-2020-0845	Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0844	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0843	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0842	Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0841	Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0840	Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0839	Windows dnsrslvr.dll Elevation of Privilege Vulnerability
CVE-2020-0838	NTFS Elevation of Privilege Vulnerability
CVE-2020-0837	ADFS Spoofing Vulnerability
CVE-2020-0836	Windows DNS Denial of Service Vulnerability
CVE-2020-0834	Windows ALPC Elevation of Privilege Vulnerability
CVE-2020-0833	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0832	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0831	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0830	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0829	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0828	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0827	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0826	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0825	Scripting Engine Memory Corruption Vulnerability
CVE-2020-0824	Internet Explorer Memory Corruption Vulnerability

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
CVE-2020-0724	Win32k Elevation of Privilege Vulnerability
CVE-2020-0723	Win32k Elevation of Privilege Vulnerability
CVE-2020-0722	Win32k Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

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
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

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

http://buildings.honeywell.com/security

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
CVE-2020-0610	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability
CVE-2020-0608	Win32k Information Disclosure Vulnerability
CVE-2020-0607	Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2020-0606	.NET Framework Remote Code Execution Vulnerability
CVE-2020-0605	.NET Framework Remote Code Execution Vulnerability
CVE-2020-0601	Windows CryptoAPI Spoofing Vulnerability

2019 – Microsoft® Patches Tested with Pro-Watch

CVE-2019-1226	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1225	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1224	Remote Desktop Protocol Server Information Disclosure Vulnerability
.NET	Quality Rollup for .NET Framework
CVE-2019-1488	Microsoft Defender Security Feature Bypass Vulnerability
CVE-2019-1485	VBScript Remote Code Execution Vulnerability
CVE-2019-1484	Windows OLE Remote Code Execution Vulnerability
CVE-2019-1483	Windows Elevation of Privilege Vulnerability
CVE-2019-1476	Windows Elevation of Privilege Vulnerability
CVE-2019-1474	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1472	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1471	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1470	Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-1469	Win32k Information Disclosure Vulnerability
CVE-2019-1468	Win32k Graphics Remote Code Execution Vulnerability
CVE-2019-1467	Windows GDI Information Disclosure Vulnerability
CVE-2019-1466	Windows GDI Information Disclosure Vulnerability
CVE-2019-1465	Windows GDI Information Disclosure Vulnerability
CVE-2019-1458	Win32k Elevation of Privilege Vulnerability
CVE-2019-1456	OpenType Font Parsing Remote Code Execution Vulnerability
CVE-2019-1453	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1439	Windows GDI Information Disclosure Vulnerability
CVE-2019-1438	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1435	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1434	Win32k Elevation of Privilege Vulnerability
CVE-2019-1433	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1432	DirectWrite Information Disclosure Vulnerability
CVE-2019-1429	Scripting Engine Memory Corruption Vulnerability
CVE-2019-1424	NetLogon Security Feature Bypass Vulnerability
CVE-2019-1422	Windows Elevation of Privilege Vulnerability
CVE-2019-1419	OpenType Font Parsing Remote Code Execution Vulnerability
CVE-2019-1418	Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2019-1415	Windows Installer Elevation of Privilege Vulnerability
CVE-2019-1412	OpenType Font Driver Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-1411	DirectWrite Information Disclosure Vulnerability
CVE-2019-1409	Windows Remote Procedure Call Information Disclosure Vulnerability
CVE-2019-1408	Win32k Elevation of Privilege Vulnerability
CVE-2019-1407	Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1406	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1405	Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2019-1399	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-1397	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1396	Win32k Elevation of Privilege Vulnerability
CVE-2019-1395	Win32k Elevation of Privilege Vulnerability
CVE-2019-1394	Win32k Elevation of Privilege Vulnerability
CVE-2019-1393	Win32k Elevation of Privilege Vulnerability
CVE-2019-1392	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1391	Windows Denial of Service Vulnerability
CVE-2019-1390	VBScript Remote Code Execution Vulnerability
CVE-2019-1389	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1388	Windows Certificate Dialog Elevation of Privilege Vulnerability
CVE-2019-1384	Microsoft Windows Security Feature Bypass Vulnerability
CVE-2019-1382	Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2019-1381	Microsoft Windows Information Disclosure Vulnerability
CVE-2019-1380	Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2019-11135	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0860	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-0838	Windows Information Disclosure Vulnerability
CVE-2019-0719	Hyper-V Remote Code Execution Vulnerability
CVE-2019-0712	Windows Hyper-V Denial of Service Vulnerability
.NET	Quality Rollup for .NET Framework
CVE-2019-1371	Internet Explorer Memory Corruption Vulnerability
CVE-2019-1368	Windows Secure Boot Security Feature Bypass Vulnerability
CVE-2019-1367	Scripting Engine Memory Corruption Vulnerability
CVE-2019-1366	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1365	Microsoft IIS Server Elevation of Privilege Vulnerability
CVE-2019-1359	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1358	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1357	Browser Spoofing Vulnerability
CVE-2019-1356	Microsoft Edge based on Edge HTML Information Disclosure Vulnerability
CVE-2019-1347	Windows Denial of Service Vulnerability
CVE-2019-1346	Windows Denial of Service Vulnerability
CVE-2019-1345	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1344	Windows Code Integrity Module Information Disclosure Vulnerability
CVE-2019-1343	Windows Denial of Service Vulnerability
CVE-2019-1342	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2019-1341	Windows Power Service Elevation of Privilege Vulnerability
CVE-2019-1340	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1339	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1337	Windows Update Client Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-1336	Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2019-1335	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1334	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1333	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1326	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1325	Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
CVE-2019-1323	Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2019-1322	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1321	Microsoft Windows CloudStore Elevation of Privilege Vulnerability
CVE-2019-1320	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1319	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2019-1318	Microsoft Windows Transport Layer Security Spoofing Vulnerability
CVE-2019-1317	Microsoft Windows Denial of Service Vulnerability
CVE-2019-1315	Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2019-1311	Windows Imaging API Remote Code Execution Vulnerability
CVE-2019-1308	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1307	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1238	VBScript Remote Code Execution Vulnerability
CVE-2019-1192	Microsoft Browsers Security Feature Bypass Vulnerability
CVE-2019-1166	Windows NTLM Tampering Vulnerability
CVE-2019-1060	MS XML Remote Code Execution Vulnerability
CVE-2019-0608	Microsoft Browser Spoofing Vulnerability
CVE-2019-0537	Microsoft Visual Studio Information Disclosure Vulnerability
.NET	Preview of Quality Rollup for .NET Framework
CVE-2019-1303	Windows Elevation of Privilege Vulnerability
CVE-2019-1300	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1299	Microsoft Edge based on Edge HTML Information Disclosure Vulnerability
CVE-2019-1298	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1294	Windows Secure Boot Security Feature Bypass Vulnerability
CVE-2019-1293	Windows SMB Client Driver Information Disclosure Vulnerability
CVE-2019-1292	Windows Elevation of Privilege Vulnerability
CVE-2019-1291	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1290	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1289	Windows Update Delivery Optimization Elevation of Privilege Vulnerability
CVE-2019-1287	Windows Network Connectivity Assistant Elevation of Privilege Vulnerability
CVE-2019-1286	Windows GDI Information Disclosure Vulnerability
CVE-2019-1285	Win32k Elevation of Privilege Vulnerability
CVE-2019-1282	Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2019-1280	LNK Remote Code Execution Vulnerability
CVE-2019-1278	Windows Elevation of Privilege Vulnerability
CVE-2019-1277	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1274	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1273	Active Directory Federation Services XSS Vulnerability
CVE-2019-1272	Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1271	Windows Media Elevation of Privilege Vulnerability
CVE-2019-1270	Microsoft Windows Store Installer Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-1269	Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1268	Winlogon Elevation of Privilege Vulnerability
CVE-2019-1267	Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability
CVE-2019-1256	Win32k Elevation of Privilege Vulnerability
CVE-2019-1254	Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-1253	Windows Elevation of Privilege Vulnerability
CVE-2019-1252	Windows GDI Information Disclosure Vulnerability
CVE-2019-1251	DirectWrite Information Disclosure Vulnerability
CVE-2019-1250	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1249	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1248	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1247	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1246	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1245	DirectWrite Information Disclosure Vulnerability
CVE-2019-1244	DirectWrite Information Disclosure Vulnerability
CVE-2019-1243	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1242	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1241	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1240	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1237	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1236	VBScript Remote Code Execution Vulnerability
CVE-2019-1235	Windows Text Service Framework Elevation of Privilege Vulnerability
CVE-2019-1232	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2019-1226	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1225	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1224	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1221	Scripting Engine Memory Corruption Vulnerability
CVE-2019-1220	Microsoft Browser Security Feature Bypass Vulnerability
CVE-2019-1219	Windows Transaction Manager Information Disclosure Vulnerability
CVE-2019-1217	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-1216	DirectX Information Disclosure Vulnerability
CVE-2019-1215	Windows Elevation of Privilege Vulnerability
CVE-2019-1214	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-1208	VBScript Remote Code Execution Vulnerability
CVE-2019-1142	.NET Framework Elevation of Privilege Vulnerability
CVE-2019-1138	Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-0788	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-0787	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2018-8172	Visual Studio Remote Code Execution Vulnerability
CVE-2018-1037	Microsoft Visual Studio Information Disclosure Vulnerability
.NET	Cumulative Update for Windows 10, Windows 8.1 and Windows Server 2012 R2
CVE-2019-9518	HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9514	HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9513	HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9512	HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9511	HTTP/2 Server Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-9506	Encryption Key Negotiation of Bluetooth Vulnerability
CVE-2019-1227	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1226	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1225	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1224	Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1223	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1222	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1212	Windows DHCP Server Denial of Service Vulnerability
CVE-2019-1206	Windows DHCP Server Denial of Service Vulnerability
CVE-2019-1198	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1190	Windows Image Elevation of Privilege Vulnerability
CVE-2019-1188	LNK Remote Code Execution Vulnerability
CVE-2019-1187	XmlLite Runtime Denial of Service Vulnerability
CVE-2019-1186	Windows Elevation of Privilege Vulnerability
CVE-2019-1184	Windows Elevation of Privilege Vulnerability
CVE-2019-1183	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-1182	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1181	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-1180	Windows Elevation of Privilege Vulnerability
CVE-2019-1179	Windows Elevation of Privilege Vulnerability
CVE-2019-1178	Windows Elevation of Privilege Vulnerability
CVE-2019-1177	Windows Elevation of Privilege Vulnerability
CVE-2019-1176	DirectX Elevation of Privilege Vulnerability
CVE-2019-1175	Windows Elevation of Privilege Vulnerability
CVE-2019-1174	Windows Elevation of Privilege Vulnerability
CVE-2019-1173	Windows Elevation of Privilege Vulnerability
CVE-2019-1172	Windows Information Disclosure Vulnerability
CVE-2019-1171	SymCrypt Information Disclosure Vulnerability
CVE-2019-1170	Windows NTFS Elevation of Privilege Vulnerability
CVE-2019-1168	Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability
CVE-2019-1164	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1163	Windows File Signature Security Feature Bypass Vulnerability
CVE-2019-1162	Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1159	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1158	Windows Graphics Component Information Disclosure Vulnerability
CVE-2019-1157	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1156	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1155	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1153	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2019-1152	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1151	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1150	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1149	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1148	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2019-1147	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1146	Jet Database Engine Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-1145	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1144	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1143	Windows Graphics Component Information Disclosure Vulnerability
CVE-2019-1078	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2019-1057	MS XML Remote Code Execution Vulnerability
CVE-2019-0965	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0736	Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0723	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0720	Hyper-V Remote Code Execution Vulnerability
CVE-2019-0718	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0717	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0716	Windows Denial of Service Vulnerability
CVE-2019-0715	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0714	Windows Hyper-V Denial of Service Vulnerability
.NET	Cumulative Update for Windows 10, Windows Server 2012 R2 and Windows Server 2016
CVE-2019-1130	Windows Elevation of Privilege Vulnerability
CVE-2019-1129	Windows Elevation of Privilege Vulnerability
CVE-2019-1128	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1127	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1126	ADFS Security Feature Bypass Vulnerability
CVE-2019-1124	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1123	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1122	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1121	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1120	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1119	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1118	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1117	DirectWrite Remote Code Execution Vulnerability
CVE-2019-1113	.NET Framework Remote Code Execution Vulnerability
CVE-2019-1108	Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2019-1102	GDI+ Remote Code Execution Vulnerability
CVE-2019-1097	DirectWrite Information Disclosure Vulnerability
CVE-2019-1096	Win32k Information Disclosure Vulnerability
CVE-2019-1095	Windows GDI Information Disclosure Vulnerability
CVE-2019-1094	Windows GDI Information Disclosure Vulnerability
CVE-2019-1093	DirectWrite Information Disclosure Vulnerability
CVE-2019-1091	Microsoft unistore.dll Information Disclosure Vulnerability
CVE-2019-1090	Windows RPCSS Elevation of Privilege Vulnerability
CVE-2019-1089	Windows RPCSS Elevation of Privilege Vulnerability
CVE-2019-1088	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1087	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1086	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1085	Windows WLAN Service Elevation of Privilege Vulnerability
CVE-2019-1083	.NET Denial of Service Vulnerability
CVE-2019-1082	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1074	Microsoft Windows Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-1073	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1071	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1067	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1037	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2019-1006	WCF/WIF SAML Token Authentication Bypass Vulnerability
CVE-2019-0975	ADFS Security Feature Bypass Vulnerability
CVE-2019-0966	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0887	Remote Desktop Services Remote Code Execution Vulnerability
CVE-2019-0880	Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2019-0865	SymCrypt Denial of Service Vulnerability
CVE-2019-0811	Windows DNS Server Denial of Service Vulnerability
CVE-2019-0785	Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-0683	Active Directory Elevation of Privilege Vulnerability
.NET	Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10, version 1809
CVE-2019-1069	Task Scheduler Elevation of Privilege Vulnerability
CVE-2019-1065	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1064	Windows Elevation of Privilege Vulnerability
CVE-2019-1053	Windows Shell Elevation of Privilege Vulnerability
CVE-2019-1050	Windows GDI Information Disclosure Vulnerability
CVE-2019-1046	Windows GDI Information Disclosure Vulnerability
CVE-2019-1045	Windows Network File System Elevation of Privilege Vulnerability
CVE-2019-1044	Windows Secure Kernel Mode Security Feature Bypass Vulnerability
CVE-2019-1043	Comctl32 Remote Code Execution Vulnerability
CVE-2019-1041	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1040	Windows NTLM Tampering Vulnerability
CVE-2019-1039	Windows Kernel Information Disclosure Vulnerability
CVE-2019-1028	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1027	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1026	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1025	Windows Denial of Service Vulnerability
CVE-2019-1022	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1021	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1019	Microsoft Windows Security Feature Bypass Vulnerability
CVE-2019-1018	DirectX Elevation of Privilege Vulnerability
CVE-2019-1017	Win32k Elevation of Privilege Vulnerability
CVE-2019-1014	Win32k Elevation of Privilege Vulnerability
CVE-2019-1012	Windows GDI Information Disclosure Vulnerability
CVE-2019-1010	Windows GDI Information Disclosure Vulnerability
CVE-2019-1007	Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-0998	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0986	Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2019-0984	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-0983	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0974	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0973	Windows Installer Elevation of Privilege Vulnerability
CVE-2019-0972	Local Security Authority Subsystem Service Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-0959	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-0948	Windows Event Viewer Information Disclosure Vulnerability
CVE-2019-0943	Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-0941	Microsoft IIS Server Denial of Service Vulnerability
CVE-2019-0909	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0908	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0907	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0906	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0905	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0904	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0888	ActiveX Data Objects (ADO) Remote Code Execution Vulnerability
CVE-2019-0722	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0713	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0711	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0710	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0620	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0981	.Net Framework and .Net Core Denial of Service Vulnerability
CVE-2019-0980	.Net Framework and .Net Core Denial of Service Vulnerability
CVE-2019-0683	Active Directory Elevation of Privilege Vulnerability
CVE-2019-0961	Windows GDI Information Disclosure Vulnerability
CVE-2019-0942	Unified Write Filter Elevation of Privilege Vulnerability
CVE-2019-0936	Windows Elevation of Privilege Vulnerability
CVE-2019-0931	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0903	GDI+ Remote Code Execution Vulnerability
CVE-2019-0902	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0901	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0900	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0899	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0898	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0897	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0896	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0895	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0894	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0893	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0892	Win32k Elevation of Privilege Vulnerability
CVE-2019-0891	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0890	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0889	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0886	Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-0885	Windows OLE Remote Code Execution Vulnerability
CVE-2019-0882	Windows GDI Information Disclosure Vulnerability
CVE-2019-0881	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0864	.NET Framework Denial of Service Vulnerability
CVE-2019-0863	Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2019-0820	.NET Framework and .NET Core Denial of Service Vulnerability
CVE-2019-0758	Windows GDI Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2019-0734	Windows Elevation of Privilege Vulnerability
CVE-2019-0733	Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2019-0727	Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability
CVE-2019-0725	Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-0707	Windows NDIS Elevation of Privilege Vulnerability
.NET	No .NET Framework updates for April 2019
CVE-2019-0674	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
CVE-2019-0673	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
CVE-2019-0671	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
CVE-2019-0879	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0877	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0859	Win32k Elevation of Privilege Vulnerability
CVE-2019-0856	Windows Remote Code Execution Vulnerability
CVE-2019-0853	GDI+ Remote Code Execution Vulnerability
CVE-2019-0851	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0849	Windows GDI Information Disclosure Vulnerability
CVE-2019-0848	Win32k Information Disclosure Vulnerability
CVE-2019-0847	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0846	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0845	Windows IOleCvt Interface Remote Code Execution Vulnerability
CVE-2019-0844	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0842	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0841	Windows Elevation of Privilege Vulnerability
CVE-2019-0840	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0839	Windows Information Disclosure Vulnerability
CVE-2019-0838	Windows Information Disclosure Vulnerability
CVE-2019-0836	Windows Elevation of Privilege Vulnerability
CVE-2019-0814	Win32k Information Disclosure Vulnerability
CVE-2019-0805	Windows Elevation of Privilege Vulnerability
CVE-2019-0803	Win32k Elevation of Privilege Vulnerability
CVE-2019-0802	Windows GDI Information Disclosure Vulnerability
CVE-2019-0796	Windows Elevation of Privilege Vulnerability
CVE-2019-0795	MS XML Remote Code Execution Vulnerability
CVE-2019-0794	OLE Automation Remote Code Execution Vulnerability
CVE-2019-0793	MS XML Remote Code Execution Vulnerability
CVE-2019-0792	MS XML Remote Code Execution Vulnerability
CVE-2019-0791	MS XML Remote Code Execution Vulnerability
CVE-2019-0790	MS XML Remote Code Execution Vulnerability
CVE-2019-0786	Hyper-V vSMB Remote Code Execution Vulnerability
CVE-2019-0735	Windows CSRSS Elevation of Privilege Vulnerability
CVE-2019-0732	Windows Security Feature Bypass Vulnerability
CVE-2019-0731	Windows Elevation of Privilege Vulnerability
CVE-2019-0730	Windows Elevation of Privilege Vulnerability
CVE-2019-0688	Windows TCP/IP Information Disclosure Vulnerability
CVE-2019-0685	Win32k Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

.NET	No .NET Framework updates for March 2019
CVE-2019-0601	HID Information Disclosure Vulnerability
CVE-2019-0821	Windows SMB Information Disclosure Vulnerability
CVE-2019-0797	Win32k Elevation of Privilege Vulnerability
CVE-2019-0784	Windows ActiveX Remote Code Execution Vulnerability
CVE-2019-0782	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0776	Win32k Information Disclosure Vulnerability
CVE-2019-0775	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0774	Windows GDI Information Disclosure Vulnerability
CVE-2019-0772	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0767	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0766	Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-0765	Comctl32 Remote Code Execution Vulnerability
CVE-2019-0759	Windows Print Spooler Information Disclosure Vulnerability
CVE-2019-0756	MS XML Remote Code Execution Vulnerability
CVE-2019-0755	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0754	Windows Denial of Service Vulnerability
CVE-2019-0726	Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0704	Windows SMB Information Disclosure Vulnerability
CVE-2019-0703	Windows SMB Information Disclosure Vulnerability
CVE-2019-0702	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0701	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0698	Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0697	Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0696	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0695	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0694	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0693	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0692	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0690	Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0689	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0682	Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0617	Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0614	Windows GDI Information Disclosure Vulnerability
CVE-2019-0603	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
CVE-2019-0664	Windows GDI Information Disclosure Vulnerability
CVE-2019-0663	Windows Kernel Information Disclosure Vulnerability
CVE-2019-0662	GDI+ Remote Code Execution Vulnerability
CVE-2019-0660	Windows GDI Information Disclosure Vulnerability
CVE-2019-0659	Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0656	Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0637	Windows Defender Firewall Security Feature Bypass Vulnerability
CVE-2019-0636	Windows Information Disclosure Vulnerability
CVE-2019-0635	Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-0633	Windows SMB Remote Code Execution Vulnerability
CVE-2019-0632	Windows Security Feature Bypass Vulnerability

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

http://buildings.honeywell.com/security

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

2018 – Microsoft® Patches Tested with Pro-Watch

CVE-2018-0859	Scripting Engine Memory Corruption Vulnerability
CVE-2018-12207	Windows Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-8641	Win32k Elevation of Privilege Vulnerability
CVE-2018-8639	Win32k Elevation of Privilege Vulnerability
CVE-2018-8637	Win32k Information Disclosure Vulnerability
CVE-2018-8634	Microsoft Text-To-Speech Remote Code Execution Vulnerability
CVE-2018-8626	Windows DNS Server Heap Overflow Vulnerability
CVE-2018-8622	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8612	Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2018-8611	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8599	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2018-8596	Windows GDI Information Disclosure Vulnerability
CVE-2018-8595	Windows GDI Information Disclosure Vulnerability
CVE-2018-8514	Remote Procedure Call runtime Information Disclosure Vulnerability
CVE-2018-8477	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8584	Windows ALPC Elevation of Privilege Vulnerability
CVE-2018-8565	Win32k Information Disclosure Vulnerability
CVE-2018-8563	DirectX Information Disclosure Vulnerability
CVE-2018-8562	Win32k Elevation of Privilege Vulnerability
CVE-2018-8561	DirectX Elevation of Privilege Vulnerability
CVE-2018-8554	DirectX Elevation of Privilege Vulnerability
CVE-2018-8553	Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2018-8552	Scripting Engine Memory Corruption Vulnerability
CVE-2018-8550	Windows COM Elevation of Privilege Vulnerability
CVE-2018-8549	Windows Security Feature Bypass Vulnerability
CVE-2018-8547	Active Directory Federation Services XSS Vulnerability
CVE-2018-8544	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-8485	DirectX Elevation of Privilege Vulnerability
CVE-2018-8476	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
CVE-2018-8471	Microsoft RemoteFX Virtual GPU miniport driver Elevation of Privilege Vulnerability
CVE-2018-8454	Windows Audio Service Information Disclosure Vulnerability
CVE-2018-8450	Windows Search Remote Code Execution Vulnerability
CVE-2018-8417	Microsoft JScript Security Feature Bypass Vulnerability
CVE-2018-8415	Microsoft PowerShell Tampering Vulnerability
CVE-2018-8408	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8407	Remote Procedure Call runtime Information Disclosure Vulnerability
CVE-2018-8256	Microsoft PowerShell Remote Code Execution Vulnerability
CVE-2018-8506	Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2018-8497	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8495	Windows Shell Remote Code Execution Vulnerability
CVE-2018-8494	MS XML Remote Code Execution Vulnerability
CVE-2018-8493	Windows TCP/IP Information Disclosure Vulnerability
CVE-2018-8492	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8489	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8486	DirectX Information Disclosure Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-8484	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8482	Windows Media Player Information Disclosure Vulnerability
CVE-2018-8481	Windows Media Player Information Disclosure Vulnerability
CVE-2018-8472	Windows GDI Information Disclosure Vulnerability
CVE-2018-8453	Win32k Elevation of Privilege Vulnerability
CVE-2018-8423	Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8413	Windows Theme API Remote Code Execution Vulnerability
CVE-2018-8411	NTFS Elevation of Privilege Vulnerability
CVE-2018-8333	Microsoft Filter Manager Elevation Of Privilege Vulnerability
CVE-2018-8330	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8329	Linux On Windows Elevation Of Privilege Vulnerability
CVE-2018-8320	Windows DNS Security Feature Bypass Vulnerability
CVE-2018-8475	Windows Remote Code Execution Vulnerability
CVE-2018-8468	Windows Elevation of Privilege Vulnerability
CVE-2018-8455	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8446	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8444	Windows SMB Information Disclosure Vulnerability
CVE-2018-8443	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8442	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8440	Windows ALPC Elevation of Privilege Vulnerability
CVE-2018-8439	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8438	Windows Hyper-V Denial of Service Vulnerability
CVE-2018-8434	Windows Hyper-V Information Disclosure Vulnerability
CVE-2018-8433	Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2018-8424	Windows GDI Information Disclosure Vulnerability
CVE-2018-8420	MS XML Remote Code Execution Vulnerability
CVE-2018-8419	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8410	Windows Registry Elevation of Privilege Vulnerability
CVE-2018-8393	Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8392	Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8335	Windows SMB Denial of Service Vulnerability
CVE-2018-8332	Win32k Graphics Remote Code Execution Vulnerability
CVE-2018-8271	Windows Information Disclosure Vulnerability
CVE-2018-8414	Windows Shell Remote Code Execution Vulnerability
CVE-2018-8406	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8405	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8404	Win32k Elevation of Privilege Vulnerability
CVE-2018-8401	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8400	DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8399	Win32k Elevation of Privilege Vulnerability
CVE-2018-8398	Windows GDI Information Disclosure Vulnerability
CVE-2018-8394	Windows GDI Information Disclosure Vulnerability
CVE-2018-8360	.NET Framework Information Disclosure Vulnerability
CVE-2018-8350	Windows PDF Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-8349	Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2018-8348	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8347	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8345	LNK Remote Code Execution Vulnerability
CVE-2018-8344	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-8343	Windows NDIS Elevation of Privilege Vulnerability
CVE-2018-8341	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8340	AD FS Security Feature Bypass Vulnerability
CVE-2018-8339	Windows Installer Elevation of Privilege Vulnerability
CVE-2018-8204	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8202	.NET Framework Elevation of Privilege Vulnerability
CVE-2018-8200	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-0952	Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2018-8356	.NET Framework Security Feature Bypass Vulnerability
CVE-2018-8314	Windows Elevation of Privilege Vulnerability
CVE-2018-8313	Windows Elevation of Privilege Vulnerability
CVE-2018-8309	Windows Denial of Service Vulnerability
CVE-2018-8308	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8307	WordPad Security Feature Bypass Vulnerability
CVE-2018-8304	Windows DNSAPI Denial of Service Vulnerability
CVE-2018-8284	.NET Framework Remote Code Injection Vulnerability
CVE-2018-8282	Win32k Elevation of Privilege Vulnerability
CVE-2018-8260	.NET Framework Remote Code Execution Vulnerability
CVE-2018-8242	Scripting Engine Memory Corruption Vulnerability
CVE-2018-8222	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8206	Windows FTP Server Denial of Service Vulnerability
CVE-2018-8202	.NET Framework Elevation of Privilege Vulnerability
CVE-2018-8251	Media Foundation Memory Corruption Vulnerability
CVE-2018-8239	Windows GDI Information Disclosure Vulnerability
CVE-2018-8233	Win32k Elevation of Privilege Vulnerability
CVE-2018-8231	HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2018-8226	HTTP.sys Denial of Service Vulnerability
CVE-2018-8225	Windows DNSAPI Remote Code Execution Vulnerability
CVE-2018-8221	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8219	Hypervisor Code Integrity Elevation of Privilege Vulnerability
CVE-2018-8215	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8214	Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-8213	Windows Remote Code Execution Vulnerability
CVE-2018-8212	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8211	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8210	Windows Remote Code Execution Vulnerability
CVE-2018-8208	Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-8207	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8205	Windows Denial of Service Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-8201	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8175	WEBDAV Denial of Service Vulnerability
CVE-2018-8169	HIDParser Elevation of Privilege Vulnerability
CVE-2018-8140	Cortana Elevation of Privilege Vulnerability
CVE-2018-8121	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0982	Windows Elevation of Privilege Vulnerability
CVE-2018-1040	Windows Code Integrity Module Denial of Service Vulnerability
CVE-2018-1036	NTFS Elevation of Privilege Vulnerability
CVE-2018-1003	Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8897	Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8174	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-8167	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2018-8166	Win32k Elevation of Privilege Vulnerability
CVE-2018-8164	Win32k Elevation of Privilege Vulnerability
CVE-2018-8136	Windows Remote Code Execution Vulnerability
CVE-2018-8134	Windows Elevation of Privilege Vulnerability
CVE-2018-8127	Windows Kernel Information Disclosure Vulnerability
CVE-2018-8124	Win32k Elevation of Privilege Vulnerability
CVE-2018-0959	Hyper-V Remote Code Execution Vulnerability
CVE-2018-0824	Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2018-8116	Microsoft Graphics Component Denial of Service Vulnerability
CVE-2018-1035	Windows Security Feature Bypass Vulnerability
CVE-2018-1016	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1015	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1013	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1012	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1010	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1009	Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2018-1008	Graphics Component Font Parsing Elevation of Privilege Vulnerability
CVE-2018-1004	Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-1003	Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-0976	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2018-0975	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0974	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0973	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0972	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0971	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0970	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0969	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0968	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0967	Windows SNMP Service Denial of Service Vulnerability
CVE-2018-0966	Device Guard Security Feature Bypass Vulnerability
CVE-2018-0964	Hyper-V Information Disclosure Vulnerability
CVE-2018-0963	Windows Kernel Elevation of Privilege Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-0960	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0957	Hyper-V Information Disclosure Vulnerability
CVE-2018-0956	HTTP.sys Denial of Service Vulnerability
CVE-2018-0890	Active Directory Security Feature Bypass Vulnerability
CVE-2018-0887	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0983	Windows Storage Services Elevation of Privilege Vulnerability
CVE-2018-0977	Win32k Elevation of Privilege Vulnerability
CVE-2018-0926	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0904	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0901	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0900	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0899	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0898	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0897	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0896	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0895	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0894	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0888	Hyper-V Information Disclosure Vulnerability
CVE-2018-0886	CredSSP Remote Code Execution Vulnerability
CVE-2018-0885	Windows Hyper-V Denial of Service Vulnerability
CVE-2018-0884	Windows Security Feature Bypass Vulnerability
CVE-2018-0883	Windows Shell Remote Code Execution Vulnerability
CVE-2018-0881	Microsoft Video Control Elevation of Privilege Vulnerability
CVE-2018-0880	Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-0878	Windows Remote Assistance Information Disclosure Vulnerability
CVE-2018-0868	Windows Installer Elevation of Privilege Vulnerability
CVE-2018-0817	Windows GDI Elevation of Privilege Vulnerability
CVE-2018-0816	Windows GDI Elevation of Privilege Vulnerability
CVE-2018-0814	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0813	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0811	Windows Kernel Information Disclosure Vulnerability
CVE-2018-0800	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0781	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0780	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0778	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0777	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0776	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0800	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0781	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0780	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0778	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0777	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0776	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0775	Scripting Engine Memory Corruption Vulnerability

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

http://buildings.honeywell.com/security

CVE-2018-0774	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0773	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0772	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0770	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0769	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0767	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0762	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0758	Scripting Engine Memory Corruption Vulnerability

2017 – Microsoft® Patches Tested with Pro-Watch

CVE-2017-11918	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11914	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11912	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11911	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11910	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11909	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11908	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11907	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11905	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11903	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11901	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11895	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11894	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11893	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11890	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11889	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11888	Microsoft Edge Memory Corruption Vulnerability
CVE-2017-11886	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11873	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11871	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11870	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11869	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11866	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11862	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11861	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11858	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11856	Internet Explorer Memory Corruption Vulnerability
CVE-2017-11855	Internet Explorer Memory Corruption Vulnerability
CVE-2017-11846	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11845	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11843	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11841	Scripting Engine Memory Corruption Vulnerability

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

http://buildings.honeywell.com/security

CVE-2017-11840	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11839	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11838	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11837	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11836	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11822	Internet Explorer Memory Corruption Vulnerability
CVE-2017-11821	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11819	Windows Shell Remote Code Execution Vulnerability
CVE-2017-11813	Internet Explorer Memory Corruption Vulnerability
CVE-2017-11812	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11811	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11810	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11809	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11808	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11807	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11806	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11805	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11804	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11802	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11801	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11800	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11799	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11798	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11797	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11796	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11793	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11792	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11779	Windows DNSAPI Remote Code Execution Vulnerability
CVE-2017-11771	Windows Search Remote Code Execution Vulnerability
CVE-2017-11766	Microsoft Edge Memory Corruption Vulnerability
CVE-2017-11764	Scripting Engine Memory Corruption Vulnerability
CVE-2017-11763	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2017-11762	Microsoft Graphics Remote Code Execution Vulnerability
CVE-2017-8759	.NET Framework Remote Code Execution Vulnerability
CVE-2017-8750	Microsoft Browser Memory Corruption Vulnerability
CVE-2017-8749	Internet Explorer Memory Corruption Vulnerability
CVE-2017-8748	Scripting Engine Memory Corruption Vulnerability
CVE-2017-8747	Scripting Engine Memory Corruption Vulnerability
CVE-2017-8741	Scripting Engine Memory Corruption Vulnerability
CVE-2017-8740	Scripting Engine Memory Corruption Vulnerability
CVE-2017-8737	Microsoft PDF Remote Code Execution Vulnerability
CVE-2017-8734	Microsoft Edge Memory Corruption Vulnerability
CVE-2017-8728	Microsoft PDF Remote Code Execution Vulnerability

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

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

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

http://buildings.honeywell.com/security

2016 – Microsoft® Patches Tested with Pro-Watch

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

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

http://buildings.honeywell.com/security

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

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

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)

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

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)

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

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)

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

http://buildings.honeywell.com/security

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

2014 – Microsoft® Patches Tested with Pro-Watch

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

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

http://buildings.honeywell.com/security

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

2013 – Microsoft® Patches Tested with Pro-Watch

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

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

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)

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

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)

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

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)

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

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)

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

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)

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

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)

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

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

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

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)

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

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)

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

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)

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

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

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

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

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

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)