

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021
<https://www.security.honeywell.com>

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-2019-1303. Patches not listed below are not applicable to a Pro-Watch system.

2019 – Microsoft® Patches Tested with Pro-Watch

| | |
|-------------------------------|--|
| .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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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-2019-1221 | 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 |
| CVE-2019-9506 | Encryption Key Negotiation of Bluetooth Vulnerability |
| CVE-2019-1227 | Windows Kernel Information Disclosure Vulnerability |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| .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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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-2018-8641 | 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|--------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|--------------------------------|--|
| 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 |
| 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 |

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 |
| 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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|-------------------------------|---|
| 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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021
<https://www.security.honeywell.com>

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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

| | |
|--------------------------|--|
| 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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021
<https://www.security.honeywell.com>

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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

(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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021
<https://www.security.honeywell.com>

[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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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 Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<https://www.security.honeywell.com>

- [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)

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021
<https://www.security.honeywell.com>

Microsoft® Service Packs tested with Pro-Watch

WINDOWS 7

[Microsoft Windows 7 Service Pack 1](#)

Windows 10 Enterprise

Not Available

WINDOWS SERVER 2008 R2

[Microsoft Windows 2008 R2 Service Pack 1](#)

WINDOWS SERVER 2012

Not Available

WINDOWS SERVER 2012 R2

Not Available

WINDOWS 8.1

Not Available

SQL SERVER 2008 R2

[Microsoft SQL Server 2008 R2 Service Pack 1](#)

[Microsoft SQL Server 2008 R2 Service Pack 2](#)

[Microsoft SQL Server 2008 R2 Service Pack 3](#)

SQL SERVER 2012

[Microsoft SQL Server 2012 Service Pack 1](#)

[Microsoft SQL Server 2012 Service Pack 2](#)

[Microsoft SQL Server 2012 Service Pack 3](#)

[Microsoft SQL Server 2012 Service Pack 4](#)

** If using Windows 7 on a standalone Pro-Watch Professional Installation, ports 1433 and 445 need to be opened on the Windows Firewall.