

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-2022-2481/CVE-2022-35798](#), patches not listed below are not applicable to a Pro-Watch system.

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

|                                |                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------|
| <a href="#">CVE-2022-35798</a> | Azure Arc Jumpstart Information Disclosure Vulnerability                                    |
| <a href="#">CVE-2022-33680</a> | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-33672</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33671</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33669</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33668</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33667</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33666</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33665</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33664</a> | Azure Site Recovery Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-33639</a> | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-33638</a> | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-32230</a> | Windows SMB Denial of Service Vulnerability                                                 |
| <a href="#">CVE-2022-30193</a> | AV1 Video Extension Remote Code Execution Vulnerability                                     |
| <a href="#">CVE-2022-30192</a> | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-30188</a> | HEVC Video Extensions Remote Code Execution Vulnerability                                   |
| <a href="#">CVE-2022-30184</a> | .NET and Visual Studio Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2022-30180</a> | Azure RTOS GUIX Studio Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2022-30179</a> | Azure RTOS GUIX Studio Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2022-30177</a> | Azure RTOS GUIX Studio Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2022-30166</a> | Local Security Authority Subsystem Service Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2022-30165</a> | Windows Kerberos Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2022-30164</a> | Kerberos AppContainer Security Feature Bypass Vulnerability                                 |
| <a href="#">CVE-2022-30163</a> | Windows Hyper-V Remote Code Execution Vulnerability                                         |
| <a href="#">CVE-2022-30162</a> | Windows Kernel Information Disclosure Vulnerability                                         |
| <a href="#">CVE-2022-30161</a> | Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability    |
| <a href="#">CVE-2022-30160</a> | Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2022-30155</a> | Windows Kernel Denial of Service Vulnerability                                              |
| <a href="#">CVE-2022-30154</a> | Microsoft File Server Shadow Copy Agent Service (RVSS) Elevation of Privilege Vulnerability |
| <a href="#">CVE-2022-30153</a> | Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability    |
| <a href="#">CVE-2022-30138</a> | Windows Print Spooler Elevation of Privilege Vulnerability                                  |
| <a href="#">CVE-2022-30130</a> | .NET Framework Denial of Service Vulnerability                                              |

|                                |                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2022-29149</a> | Azure Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability                                              |
| <a href="#">CVE-2022-29143</a> | Microsoft SQL Server Remote Code Execution Vulnerability                                                                     |
| <a href="#">CVE-2022-29142</a> | Windows Kernel Elevation of Privilege Vulnerability                                                                          |
| <a href="#">CVE-2022-29141</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29140</a> | Windows Print Spooler Information Disclosure Vulnerability                                                                   |
| <a href="#">CVE-2022-29139</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29138</a> | Windows Clustered Shared Volume Elevation of Privilege Vulnerability                                                         |
| <a href="#">CVE-2022-29137</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29135</a> | Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability                                                     |
| <a href="#">CVE-2022-29134</a> | Windows Clustered Shared Volume Information Disclosure Vulnerability                                                         |
| <a href="#">CVE-2022-29132</a> | Windows Print Spooler Elevation of Privilege Vulnerability                                                                   |
| <a href="#">CVE-2022-29131</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29130</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29129</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-29128</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-27776</a> | HackerOne: CVE-2022-27776 Insufficiently protected credentials vulnerability might leak authentication or cookie header data |
| <a href="#">CVE-2022-26920</a> | Windows Graphics Component Information Disclosure Vulnerability                                                              |
| <a href="#">CVE-2022-26919</a> | Windows LDAP Remote Code Execution Vulnerability                                                                             |
| <a href="#">CVE-2022-26918</a> | Windows Fax Compose Form Remote Code Execution Vulnerability                                                                 |
| <a href="#">CVE-2022-26917</a> | Windows Fax Compose Form Remote Code Execution Vulnerability                                                                 |
| <a href="#">CVE-2022-26916</a> | Windows Fax Compose Form Remote Code Execution Vulnerability                                                                 |
| <a href="#">CVE-2022-26915</a> | Windows Secure Channel Denial of Service Vulnerability                                                                       |
| <a href="#">CVE-2022-26904</a> | Windows User Profile Service Elevation of Privilege Vulnerability                                                            |
| <a href="#">CVE-2022-26832</a> | .NET Framework Denial of Service Vulnerability                                                                               |
| <a href="#">CVE-2022-26831</a> | Windows LDAP Denial of Service Vulnerability                                                                                 |
| <a href="#">CVE-2022-26828</a> | Windows Bluetooth Driver Elevation of Privilege Vulnerability                                                                |
| <a href="#">CVE-2022-26827</a> | Windows File Server Resource Management Service Elevation of Privilege Vulnerability                                         |
| <a href="#">CVE-2022-26825</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26824</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26823</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26822</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26821</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26812</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26811</a> | Windows DNS Server Remote Code Execution Vulnerability                                                                       |
| <a href="#">CVE-2022-26810</a> | Windows File Server Resource Management Service Elevation of Privilege Vulnerability                                         |
| <a href="#">CVE-2022-26809</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                                                            |
| <a href="#">CVE-2022-26808</a> | Windows File Explorer Elevation of Privilege Vulnerability                                                                   |
| <a href="#">CVE-2022-26807</a> | Windows Work Folder Service Elevation of Privilege Vulnerability                                                             |

|                                |                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------|
| <a href="#">CVE-2022-26803</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26802</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26801</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26798</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26797</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26796</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26794</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26792</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26790</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26789</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26787</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-26786</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-24525</a> | Windows Update Stack Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2022-24512</a> | .NET and Visual Studio Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2022-24507</a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2022-24503</a> | Remote Desktop Protocol Client Information Disclosure Vulnerability                  |
| <a href="#">CVE-2022-24502</a> | Windows HTML Platforms Security Feature Bypass Vulnerability                         |
| <a href="#">CVE-2022-24464</a> | .NET and Visual Studio Denial of Service Vulnerability                               |
| <a href="#">CVE-2022-24460</a> | Tablet Windows User Interface Application Elevation of Privilege Vulnerability       |
| <a href="#">CVE-2022-24459</a> | Windows Fax and Scan Service Elevation of Privilege Vulnerability                    |
| <a href="#">CVE-2022-24455</a> | Windows CD-ROM Driver Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-24454</a> | Windows Security Support Provider Interface Elevation of Privilege Vulnerability     |
| <a href="#">CVE-2022-23825</a> | AMD: CVE-2022-23825 AMD CPU Branch Type Confusion                                    |
| <a href="#">CVE-2022-23299</a> | Windows PDEV Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-23298</a> | Windows NT OS Kernel Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2022-23297</a> | Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability |
| <a href="#">CVE-2022-23296</a> | Windows Installer Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2022-23294</a> | Windows Event Tracing Remote Code Execution Vulnerability                            |
| <a href="#">CVE-2022-23293</a> | Windows Fast FAT File System Driver Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2022-23291</a> | Windows DWM Core Library Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-23290</a> | Windows Inking COM Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2022-23288</a> | Windows DWM Core Library Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2022-23287</a> | Windows ALPC Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-23285</a> | Remote Desktop Client Remote Code Execution Vulnerability                            |
| <a href="#">CVE-2022-23284</a> | Windows Print Spooler Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2022-23283</a> | Windows ALPC Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2022-23281</a> | Windows Common Log File System Driver Information Disclosure Vulnerability           |
| <a href="#">CVE-2022-23278</a> | Microsoft Defender for Endpoint Spoofing Vulnerability                               |
| <a href="#">CVE-2022-23253</a> | Point-to-Point Tunneling Protocol Denial of Service Vulnerability                    |
| <a href="#">CVE-2022-22050</a> | Windows Fax Service Elevation of Privilege Vulnerability                             |

|                                |                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------|
| <a href="#">CVE-2022-22049</a> | Windows CSRSS Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2022-22048</a> | BitLocker Security Feature Bypass Vulnerability                                          |
| <a href="#">CVE-2022-22047</a> | Windows CSRSS Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2022-22045</a> | Windows.Devices.Picker.dll Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2022-22043</a> | Windows Fast FAT File System Driver Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2022-22042</a> | Windows Hyper-V Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2022-22041</a> | Windows Print Spooler Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2022-22040</a> | Internet Information Services Dynamic Compression Module Denial of Service Vulnerability |
| <a href="#">CVE-2022-22039</a> | Windows Network File System Remote Code Execution Vulnerability                          |
| <a href="#">CVE-2022-22019</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2022-22010</a> | Media Foundation Information Disclosure Vulnerability                                    |
| <a href="#">CVE-2022-22002</a> | Windows User Account Profile Picture Denial of Service Vulnerability                     |
| <a href="#">CVE-2022-22001</a> | Windows Remote Access Connection Manager Elevation of Privilege Vulnerability            |
| <a href="#">CVE-2022-22000</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2022-21999</a> | Windows Print Spooler Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2022-21998</a> | Windows Common Log File System Driver Information Disclosure Vulnerability               |
| <a href="#">CVE-2022-21997</a> | Windows Print Spooler Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2022-21995</a> | Windows Hyper-V Remote Code Execution Vulnerability                                      |
| <a href="#">CVE-2022-21994</a> | Windows DWM Core Library Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2022-21993</a> | Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability          |
| <a href="#">CVE-2022-21992</a> | Windows Mobile Device Management Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2022-21989</a> | Windows Kernel Elevation of Privilege Vulnerability                                      |
| <a href="#">CVE-2022-21981</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2022-21977</a> | Media Foundation Information Disclosure Vulnerability                                    |
| <a href="#">CVE-2022-21963</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21962</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21961</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21960</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21959</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21958</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21928</a> | Windows Resilient File System (ReFS) Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21924</a> | Workstation Service Remote Protocol Security Feature Bypass Vulnerability                |
| <a href="#">CVE-2022-21913</a> | Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass         |
| <a href="#">CVE-2022-21911</a> | .NET Framework Denial of Service Vulnerability                                           |
| <a href="#">CVE-2022-21908</a> | Windows Installer Elevation of Privilege Vulnerability                                   |
| <a href="#">CVE-2022-21907</a> | HTTP Protocol Stack Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2022-21906</a> | Windows Defender Application Control Security Feature Bypass Vulnerability               |
| <a href="#">CVE-2022-21905</a> | Windows Hyper-V Security Feature Bypass Vulnerability                                    |
| <a href="#">CVE-2022-21904</a> | Windows GDI Information Disclosure Vulnerability                                         |
| <a href="#">CVE-2022-21903</a> | Windows GDI Elevation of Privilege Vulnerability                                         |

|                                |                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------|
| <a href="#">CVE-2022-21902</a> | Windows DWM Core Library Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2022-21901</a> | Windows Hyper-V Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2022-21900</a> | Windows Hyper-V Security Feature Bypass Vulnerability                           |
| <a href="#">CVE-2022-21899</a> | Windows Extensible Firmware Interface Security Feature Bypass Vulnerability     |
| <a href="#">CVE-2022-21898</a> | DirectX Graphics Kernel Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2022-21897</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2022-21894</a> | Secure Boot Security Feature Bypass Vulnerability                               |
| <a href="#">CVE-2022-21890</a> | Windows IKE Extension Denial of Service Vulnerability                           |
| <a href="#">CVE-2022-21889</a> | Windows IKE Extension Denial of Service Vulnerability                           |
| <a href="#">CVE-2022-21888</a> | Windows Modern Execution Server Remote Code Execution Vulnerability             |
| <a href="#">CVE-2022-21885</a> | Windows Remote Access Connection Manager Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2022-21884</a> | Local Security Authority Subsystem Service Elevation of Privilege Vulnerability |
| <a href="#">CVE-2022-21883</a> | Windows IKE Extension Denial of Service Vulnerability                           |
| <a href="#">CVE-2022-21882</a> | Win32k Elevation of Privilege Vulnerability                                     |
| <a href="#">CVE-2022-21881</a> | Windows Kernel Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2022-21880</a> | Windows GDI+ Information Disclosure Vulnerability                               |
| <a href="#">CVE-2022-21874</a> | Windows Security Center API Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2022-21843</a> | Windows IKE Extension Denial of Service Vulnerability                           |
| <a href="#">CVE-2022-2481</a>  | Chromium: CVE-2022-2481 Use after free in Views                                 |
| <a href="#">CVE-2022-2480</a>  | Chromium: CVE-2022-2480 Use after free in Service Worker API                    |
| <a href="#">CVE-2022-2479</a>  | Chromium: CVE-2022-2479 Insufficient validation of untrusted input in File      |
| <a href="#">CVE-2022-2478</a>  | Chromium: CVE-2022-2478 Use after free in PDF                                   |
| <a href="#">CVE-2022-2477</a>  | Chromium: CVE-2022-2477 Use after free in Guest View                            |
| <a href="#">CVE-2022-2295</a>  | Chromium: CVE-2022-2295 Type Confusion in V8                                    |
| <a href="#">CVE-2022-2294</a>  | Chromium: CVE-2022-2294 Heap buffer overflow in WebRTC                          |
| <a href="#">CVE-2022-2165</a>  | Chromium: CVE-2022-2165 Insufficient data validation in URL formatting          |
| <a href="#">CVE-2022-2164</a>  | Chromium: CVE-2022-2164 Inappropriate implementation in Extensions API          |
| <a href="#">CVE-2022-2163</a>  | Chromium: CVE-2022-2163 Use after free in Cast UI and Toolbar                   |
| <a href="#">CVE-2022-2162</a>  | Chromium: CVE-2022-2162 Insufficient policy enforcement in File System API      |
| <a href="#">CVE-2022-2161</a>  | Chromium: CVE-2022-2161 Use after free in WebApp Provider                       |
| <a href="#">CVE-2022-2160</a>  | Chromium: CVE-2022-2160 Insufficient policy enforcement in DevTools             |
| <a href="#">CVE-2022-2158</a>  | Chromium: CVE-2022-2158 Type Confusion in V8                                    |
| <a href="#">CVE-2022-2157</a>  | Chromium: CVE-2022-2157 Use after free in Interest groups                       |
| <a href="#">CVE-2022-2156</a>  | Chromium: CVE-2022-2156 Use after free in Base                                  |

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

|                                |                                                                           |
|--------------------------------|---------------------------------------------------------------------------|
| <a href="#">CVE-2021-43893</a> | Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability |
| <a href="#">CVE-2021-43883</a> | Windows Installer Elevation of Privilege Vulnerability                    |
| <a href="#">CVE-2021-43877</a> | ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability       |

|                                |                                                                                         |
|--------------------------------|-----------------------------------------------------------------------------------------|
| <a href="#">CVE-2021-43248</a> | Windows Digital Media Receiver Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2021-43247</a> | Windows TCP/IP Driver Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2021-43246</a> | Windows Hyper-V Denial of Service Vulnerability                                         |
| <a href="#">CVE-2021-43245</a> | Windows Digital TV Tuner Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2021-43244</a> | Windows Kernel Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2021-43240</a> | NTFS Set Short Name Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2021-43239</a> | Windows Recovery Environment Agent Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-43238</a> | Windows Remote Access Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2021-43237</a> | Windows Setup Elevation of Privilege Vulnerability                                      |
| <a href="#">CVE-2021-43236</a> | Microsoft Message Queuing Information Disclosure Vulnerability                          |
| <a href="#">CVE-2021-43235</a> | Storage Spaces Controller Information Disclosure Vulnerability                          |
| <a href="#">CVE-2021-43234</a> | Windows Fax Service Remote Code Execution Vulnerability                                 |
| <a href="#">CVE-2021-43233</a> | Remote Desktop Client Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2021-43232</a> | Windows Event Tracing Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2021-43231</a> | Windows NTFS Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2021-43230</a> | Windows NTFS Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2021-43229</a> | Windows NTFS Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2021-43228</a> | SymCrypt Denial of Service Vulnerability                                                |
| <a href="#">CVE-2021-43227</a> | Storage Spaces Controller Information Disclosure Vulnerability                          |
| <a href="#">CVE-2021-43226</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability              |
| <a href="#">CVE-2021-43224</a> | Windows Common Log File System Driver Information Disclosure Vulnerability              |
| <a href="#">CVE-2021-43223</a> | Windows Remote Access Connection Manager Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2021-43222</a> | Microsoft Message Queuing Information Disclosure Vulnerability                          |
| <a href="#">CVE-2021-43219</a> | DirectX Graphics Kernel File Denial of Service Vulnerability                            |
| <a href="#">CVE-2021-43217</a> | Windows Encrypting File System (EFS) Remote Code Execution Vulnerability                |
| <a href="#">CVE-2021-43216</a> | Microsoft Local Security Authority Server (lsasrv) Information Disclosure Vulnerability |
| <a href="#">CVE-2021-43215</a> | iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution           |
| <a href="#">CVE-2021-43207</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability              |
| <a href="#">CVE-2021-42291</a> | Active Directory Domain Services Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-42288</a> | Windows Hello Security Feature Bypass Vulnerability                                     |
| <a href="#">CVE-2021-42287</a> | Active Directory Domain Services Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-42285</a> | Windows Kernel Elevation of Privilege Vulnerability                                     |
| <a href="#">CVE-2021-42284</a> | Windows Hyper-V Denial of Service Vulnerability                                         |
| <a href="#">CVE-2021-42283</a> | NTFS Elevation of Privilege Vulnerability                                               |
| <a href="#">CVE-2021-42282</a> | Active Directory Domain Services Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-42279</a> | Chakra Scripting Engine Memory Corruption Vulnerability                                 |
| <a href="#">CVE-2021-42278</a> | Active Directory Domain Services Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-42275</a> | Microsoft COM for Windows Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2021-41367</a> | NTFS Elevation of Privilege Vulnerability                                               |
| <a href="#">CVE-2021-41361</a> | Active Directory Federation Server Spoofing Vulnerability                               |
| <a href="#">CVE-2021-41357</a> | Win32k Elevation of Privilege Vulnerability                                             |

|                                |                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">CVE-2021-41351</a> | Microsoft Edge (Chrome based) Spoofing on IE Mode                                         |
| <a href="#">CVE-2021-41347</a> | Windows AppX Deployment Service Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2021-41346</a> | Console Window Host Security Feature Bypass Vulnerability                                 |
| <a href="#">CVE-2021-41345</a> | Storage Spaces Controller Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2021-41343</a> | Windows Fast FAT File System Driver Information Disclosure Vulnerability                  |
| <a href="#">CVE-2021-41342</a> | Windows MSHTML Platform Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2021-41340</a> | Windows Graphics Component Remote Code Execution Vulnerability                            |
| <a href="#">CVE-2021-41339</a> | Microsoft DWM Core Library Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2021-41338</a> | Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability                 |
| <a href="#">CVE-2021-41337</a> | Active Directory Security Feature Bypass Vulnerability                                    |
| <a href="#">CVE-2021-41335</a> | Windows Kernel Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2021-41334</a> | Windows Desktop Bridge Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2021-41333</a> | Windows Print Spooler Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2021-41332</a> | Windows Print Spooler Information Disclosure Vulnerability                                |
| <a href="#">CVE-2021-41331</a> | Windows Media Audio Decoder Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2021-41330</a> | Microsoft Windows Media Foundation Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-40489</a> | Storage Spaces Controller Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2021-40488</a> | Storage Spaces Controller Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2021-40478</a> | Storage Spaces Controller Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2021-40477</a> | Windows Event Tracing Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2021-40476</a> | Windows AppContainer Elevation Of Privilege Vulnerability                                 |
| <a href="#">CVE-2021-40475</a> | Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability               |
| <a href="#">CVE-2021-40470</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2021-40469</a> | Windows DNS Server Remote Code Execution Vulnerability                                    |
| <a href="#">CVE-2021-40468</a> | Windows Bind Filter Driver Information Disclosure Vulnerability                           |
| <a href="#">CVE-2021-40467</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2021-40466</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2021-40465</a> | Windows Text Shaping Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2021-40464</a> | Windows Nearby Sharing Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2021-40463</a> | Windows NAT Denial of Service Vulnerability                                               |
| <a href="#">CVE-2021-40462</a> | Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability |
| <a href="#">CVE-2021-40461</a> | Windows Hyper-V Remote Code Execution Vulnerability                                       |
| <a href="#">CVE-2021-40460</a> | Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability               |
| <a href="#">CVE-2021-40456</a> | Windows AD FS Security Feature Bypass Vulnerability                                       |
| <a href="#">CVE-2021-40455</a> | Windows Installer Spoofing Vulnerability                                                  |
| <a href="#">CVE-2021-40454</a> | Rich Text Edit Control Information Disclosure Vulnerability                               |
| <a href="#">CVE-2021-40450</a> | Win32k Elevation of Privilege Vulnerability                                               |
| <a href="#">CVE-2021-40449</a> | Win32k Elevation of Privilege Vulnerability                                               |
| <a href="#">CVE-2021-40447</a> | Windows Print Spooler Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2021-40443</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2021-40441</a> | Windows Media Center Elevation of Privilege Vulnerability                                 |

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

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

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

|                                |                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------|
| <a href="#">CVE-2021-27095</a> | Windows Media Video Decoder Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2021-27094</a> | Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2021-27093</a> | Windows Kernel Information Disclosure Vulnerability                             |
| <a href="#">CVE-2021-27092</a> | Azure AD Web Sign-in Security Feature Bypass Vulnerability                      |
| <a href="#">CVE-2021-27090</a> | Windows Secure Kernel Mode Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-27089</a> | Microsoft Internet Messaging API Remote Code Execution Vulnerability            |
| <a href="#">CVE-2021-27088</a> | Windows Event Tracing Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2021-27086</a> | Windows Services and Controller App Elevation of Privilege Vulnerability        |
| <a href="#">CVE-2021-27079</a> | Windows Media Photo Codec Information Disclosure Vulnerability                  |
| <a href="#">CVE-2021-27072</a> | Win32k Elevation of Privilege Vulnerability                                     |
| <a href="#">CVE-2021-26442</a> | Windows HTTP.sys Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2021-26441</a> | Storage Spaces Controller Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2021-26435</a> | Windows Scripting Engine Memory Corruption Vulnerability                        |
| <a href="#">CVE-2021-26433</a> | Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability |
| <a href="#">CVE-2021-26432</a> | Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability  |
| <a href="#">CVE-2021-26426</a> | Windows User Account Profile Picture Elevation of Privilege Vulnerability       |
| <a href="#">CVE-2021-26424</a> | Windows TCP/IP Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2021-26419</a> | Scripting Engine Memory Corruption Vulnerability                                |
| <a href="#">CVE-2021-26417</a> | Windows Overlay Filter Information Disclosure Vulnerability                     |
| <a href="#">CVE-2021-26416</a> | Windows Hyper-V Denial of Service Vulnerability                                 |
| <a href="#">CVE-2021-26415</a> | Windows Installer Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2021-26414</a> | Windows DCOM Server Security Feature Bypass                                     |
| <a href="#">CVE-2021-26413</a> | Windows Installer Spoofing Vulnerability                                        |
| <a href="#">CVE-2021-24111</a> | .NET Framework Denial of Service Vulnerability                                  |
| <a href="#">CVE-2021-24103</a> | Windows Event Tracing Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2021-24102</a> | Windows Event Tracing Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2021-24098</a> | Windows Console Driver Denial of Service Vulnerability                          |
| <a href="#">CVE-2021-24086</a> | Windows TCP/IP Denial of Service Vulnerability                                  |
| <a href="#">CVE-2021-24082</a> | Microsoft.PowerShell.Utility Module WDAC Security Feature Bypass Vulnerability  |
| <a href="#">CVE-2021-24081</a> | Microsoft Windows Codecs Library Remote Code Execution Vulnerability            |
| <a href="#">CVE-2021-24076</a> | Microsoft Windows VMSwitch Information Disclosure Vulnerability                 |
| <a href="#">CVE-2021-24075</a> | Windows Network File System Denial of Service Vulnerability                     |
| <a href="#">CVE-2021-24106</a> | Windows DirectX Information Disclosure Vulnerability                            |
| <a href="#">CVE-2021-24096</a> | Windows Kernel Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-24094</a> | Windows TCP/IP Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2021-24093</a> | Windows Graphics Component Remote Code Execution Vulnerability                  |
| <a href="#">CVE-2021-24091</a> | Windows Camera Codec Pack Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2021-24088</a> | Windows Local Spooler Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2021-25195</a> | Windows PKU2U Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2021-24084</a> | Windows Mobile Device Management Information Disclosure Vulnerability           |
| <a href="#">CVE-2021-24083</a> | Windows Address Book Remote Code Execution Vulnerability                        |

|                                |                                                                            |
|--------------------------------|----------------------------------------------------------------------------|
| <a href="#">CVE-2021-24080</a> | Windows Trust Verification API Denial of Service Vulnerability             |
| <a href="#">CVE-2021-24079</a> | Windows Backup Engine Information Disclosure Vulnerability                 |
| <a href="#">CVE-2021-24078</a> | Windows DNS Server Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2021-24077</a> | Windows Fax Service Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-24074</a> | Windows TCP/IP Remote Code Execution Vulnerability                         |
| <a href="#">CVE-2021-1734</a>  | Windows Remote Procedure Call Information Disclosure Vulnerability         |
| <a href="#">CVE-2021-1732</a>  | Windows Win32k Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2021-1731</a>  | PFX Encryption Security Feature Bypass Vulnerability                       |
| <a href="#">CVE-2021-1727</a>  | Windows Installer Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2021-1722</a>  | Windows Fax Service Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1710</a>  | Microsoft Windows Media Foundation Remote Code Execution Vulnerability     |
| <a href="#">CVE-2021-1709</a>  | Windows Win32k Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2021-1708</a>  | Windows GDI+ Information Disclosure Vulnerability                          |
| <a href="#">CVE-2021-1706</a>  | Windows LUAFV Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2021-1705</a>  | Microsoft Edge (HTML-based) Memory Corruption Vulnerability                |
| <a href="#">CVE-2021-1704</a>  | Windows Hyper-V Elevation of Privilege Vulnerability                       |
| <a href="#">CVE-2021-1703</a>  | Windows Event Logging Service Elevation of Privilege Vulnerability         |
| <a href="#">CVE-2021-1702</a>  | Windows Remote Procedure Call Runtime Elevation of Privilege Vulnerability |
| <a href="#">CVE-2021-1701</a>  | Remote Procedure Call Runtime Remote Code Execution Vulnerability          |
| <a href="#">CVE-2021-1700</a>  | Remote Procedure Call Runtime Remote Code Execution Vulnerability          |
| <a href="#">CVE-2021-1699</a>  | Windows (modem.sys) Information Disclosure Vulnerability                   |
| <a href="#">CVE-2021-1698</a>  | Windows Win32k Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2021-1697</a>  | Windows InstallService Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2021-1696</a>  | Windows Graphics Component Information Disclosure Vulnerability            |
| <a href="#">CVE-2021-1695</a>  | Windows Print Spooler Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-1694</a>  | Windows Update Stack Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2021-1693</a>  | Windows CSC Service Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-1692</a>  | Hyper-V Denial of Service Vulnerability                                    |
| <a href="#">CVE-2021-1691</a>  | Hyper-V Denial of Service Vulnerability                                    |
| <a href="#">CVE-2021-1690</a>  | Windows WalletService Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-1689</a>  | Windows Multipoint Management Elevation of Privilege Vulnerability         |
| <a href="#">CVE-2021-1688</a>  | Windows CSC Service Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2021-1687</a>  | Windows WalletService Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-1686</a>  | Windows WalletService Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-1685</a>  | Windows AppX Deployment Extensions Elevation of Privilege Vulnerability    |
| <a href="#">CVE-2021-1684</a>  | Windows Bluetooth Security Feature Bypass Vulnerability                    |
| <a href="#">CVE-2021-1683</a>  | Windows Bluetooth Security Feature Bypass Vulnerability                    |
| <a href="#">CVE-2021-1682</a>  | Windows Kernel Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2021-1681</a>  | Windows WalletService Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2021-1680</a>  | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability    |
| <a href="#">CVE-2021-1679</a>  | Windows CryptoAPI Denial of Service Vulnerability                          |

|                               |                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------|
| <a href="#">CVE-2021-1678</a> | NTLM Security Feature Bypass Vulnerability                                           |
| <a href="#">CVE-2021-1676</a> | Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability |
| <a href="#">CVE-2021-1674</a> | Windows Remote Desktop Protocol Core Security Feature Bypass Vulnerability           |
| <a href="#">CVE-2021-1673</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1672</a> | Windows Projected File System FS Filter Driver Information Disclosure Vulnerability  |
| <a href="#">CVE-2021-1671</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1670</a> | Windows Projected File System FS Filter Driver Information Disclosure Vulnerability  |
| <a href="#">CVE-2021-1669</a> | Windows Remote Desktop Security Feature Bypass Vulnerability                         |
| <a href="#">CVE-2021-1668</a> | Microsoft DTV-DVD Video Decoder Remote Code Execution Vulnerability                  |
| <a href="#">CVE-2021-1667</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1666</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1665</a> | GDI+ Remote Code Execution Vulnerability                                             |
| <a href="#">CVE-2021-1664</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1663</a> | Windows Projected File System FS Filter Driver Information Disclosure Vulnerability  |
| <a href="#">CVE-2021-1662</a> | Windows Event Tracing Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2021-1661</a> | Windows Installer Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2021-1660</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1659</a> | Windows CSC Service Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-1658</a> | Remote Procedure Call Runtime Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2021-1657</a> | Windows Fax Compose Form Remote Code Execution Vulnerability                         |
| <a href="#">CVE-2021-1656</a> | TPM Device Driver Information Disclosure Vulnerability                               |
| <a href="#">CVE-2021-1655</a> | Windows CSC Service Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-1654</a> | Windows CSC Service Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-1653</a> | Windows CSC Service Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-1652</a> | Windows CSC Service Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2021-1651</a> | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability              |
| <a href="#">CVE-2021-1650</a> | Windows Runtime C++ Template Library Elevation of Privilege Vulnerability            |
| <a href="#">CVE-2021-1649</a> | Active Template Library Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2021-1648</a> | Microsoft splwow64 Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2021-1646</a> | Windows WLAN Service Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2021-1645</a> | Windows Docker Information Disclosure Vulnerability                                  |
| <a href="#">CVE-2021-1642</a> | Windows AppX Deployment Extensions Elevation of Privilege Vulnerability              |
| <a href="#">CVE-2021-1640</a> | Windows Elevation of Privilege Vulnerability                                         |
| <a href="#">CVE-2021-1638</a> | Windows Bluetooth Security Feature Bypass Vulnerability                              |
| <a href="#">CVE-2021-1637</a> | Windows DNS Query Information Disclosure Vulnerability                               |
| <a href="#">CVE-2021-1636</a> | Microsoft SQL Elevation of Privilege Vulnerability                                   |

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

|                                |                                                    |
|--------------------------------|----------------------------------------------------|
| <a href="#">CVE-2020-24588</a> | Windows Wireless Networking Spoofing Vulnerability |
|--------------------------------|----------------------------------------------------|

|                |                                                                             |
|----------------|-----------------------------------------------------------------------------|
| CVE-2020-17140 | Windows SMB Information Disclosure Vulnerability                            |
| CVE-2020-17139 | Windows Overlay Filter Security Feature Bypass Vulnerability                |
| CVE-2020-17138 | Windows Error Reporting Information Disclosure Vulnerability                |
| CVE-2020-17137 | DirectX Graphics Kernel Elevation of Privilege Vulnerability                |
| CVE-2020-17136 | Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability |
| CVE-2020-17134 | Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability |
| CVE-2020-17131 | Chakra Scripting Engine Memory Corruption Vulnerability                     |
| CVE-2020-17113 | Windows Camera Codec Information Disclosure Vulnerability                   |
| CVE-2020-17103 | Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability |
| CVE-2020-17099 | Windows Lock Screen Security Feature Bypass Vulnerability                   |
| CVE-2020-17098 | Windows GDI+ Information Disclosure Vulnerability                           |
| CVE-2020-17097 | Windows Digital Media Receiver Elevation of Privilege Vulnerability         |
| CVE-2020-17096 | Windows NTFS Remote Code Execution Vulnerability                            |
| CVE-2020-17095 | Hyper-V Remote Code Execution Vulnerability                                 |
| CVE-2020-17094 | Windows Error Reporting Information Disclosure Vulnerability                |
| CVE-2020-17092 | Windows Network Connections Service Elevation of Privilege Vulnerability    |
| CVE-2020-17090 | Microsoft Defender for Endpoint Security Feature Bypass Vulnerability       |
| CVE-2020-17088 | Windows Common Log File System Driver Elevation of Privilege Vulnerability  |
| CVE-2020-17088 | Windows Common Log File System Driver Elevation of Privilege Vulnerability  |
| CVE-2020-17087 | Windows Kernel Local Elevation of Privilege Vulnerability                   |
| CVE-2020-17087 | Windows Kernel Local Elevation of Privilege Vulnerability                   |
| CVE-2020-17077 | Windows Update Stack Elevation of Privilege Vulnerability                   |
| CVE-2020-17076 | Windows Update Orchestrator Service Elevation of Privilege Vulnerability    |
| CVE-2020-17075 | Windows USO Core Worker Elevation of Privilege Vulnerability                |
| CVE-2020-17074 | Windows Update Orchestrator Service Elevation of Privilege Vulnerability    |
| CVE-2020-17073 | Windows Update Orchestrator Service Elevation of Privilege Vulnerability    |
| CVE-2020-17071 | Windows Delivery Optimization Information Disclosure Vulnerability          |
| CVE-2020-17070 | Windows Update Medic Service Elevation of Privilege Vulnerability           |
| CVE-2020-17069 | Windows NDIS Information Disclosure Vulnerability                           |
| CVE-2020-17069 | Windows NDIS Information Disclosure Vulnerability                           |
| CVE-2020-17068 | Windows GDI+ Remote Code Execution Vulnerability                            |
| CVE-2020-17068 | Windows GDI+ Remote Code Execution Vulnerability                            |
| CVE-2020-17058 | Microsoft Browser Memory Corruption Vulnerability                           |
| CVE-2020-17057 | Windows Win32k Elevation of Privilege Vulnerability                         |
| CVE-2020-17056 | Windows Network File System Information Disclosure Vulnerability            |
| CVE-2020-17056 | Windows Network File System Information Disclosure Vulnerability            |
| CVE-2020-17055 | Windows Remote Access Elevation of Privilege Vulnerability                  |
| CVE-2020-17055 | Windows Remote Access Elevation of Privilege Vulnerability                  |
| CVE-2020-17054 | Chakra Scripting Engine Memory Corruption Vulnerability                     |
| CVE-2020-17053 | Internet Explorer Memory Corruption Vulnerability                           |
| CVE-2020-17052 | Scripting Engine Memory Corruption Vulnerability                            |
| CVE-2020-17052 | Scripting Engine Memory Corruption Vulnerability                            |

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| CVE-2020-17051 | Windows Network File System Remote Code Execution Vulnerability               |
| CVE-2020-17051 | Windows Network File System Remote Code Execution Vulnerability               |
| CVE-2020-17049 | Kerberos KDC Security Feature Bypass Vulnerability                            |
| CVE-2020-17049 | Kerberos KDC Security Feature Bypass Vulnerability                            |
| CVE-2020-17048 | Chakra Scripting Engine Memory Corruption Vulnerability                       |
| CVE-2020-17047 | Windows Network File System Denial of Service Vulnerability                   |
| CVE-2020-17047 | Windows Network File System Denial of Service Vulnerability                   |
| CVE-2020-17046 | Windows Error Reporting Denial of Service Vulnerability                       |
| CVE-2020-17045 | Windows KernelStream Information Disclosure Vulnerability                     |
| CVE-2020-17045 | Windows KernelStream Information Disclosure Vulnerability                     |
| CVE-2020-17044 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17044 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17043 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17043 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17042 | Windows Print Spooler Remote Code Execution Vulnerability                     |
| CVE-2020-17042 | Windows Print Spooler Remote Code Execution Vulnerability                     |
| CVE-2020-17041 | Windows Print Configuration Elevation of Privilege Vulnerability              |
| CVE-2020-17041 | Windows Print Configuration Elevation of Privilege Vulnerability              |
| CVE-2020-17040 | Windows Hyper-V Security Feature Bypass Vulnerability                         |
| CVE-2020-17040 | Windows Hyper-V Security Feature Bypass Vulnerability                         |
| CVE-2020-17038 | Win32k Elevation of Privilege Vulnerability                                   |
| CVE-2020-17038 | Win32k Elevation of Privilege Vulnerability                                   |
| CVE-2020-17037 | Windows WalletService Elevation of Privilege Vulnerability                    |
| CVE-2020-17036 | Windows Function Discovery SSDP Provider Information Disclosure Vulnerability |
| CVE-2020-17036 | Windows Function Discovery SSDP Provider Information Disclosure Vulnerability |
| CVE-2020-17035 | Windows Kernel Elevation of Privilege Vulnerability                           |
| CVE-2020-17034 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17034 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17033 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17033 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17032 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17032 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17031 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17031 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17030 | Windows MSCTF Server Information Disclosure Vulnerability                     |
| CVE-2020-17029 | Windows Canonical Display Driver Information Disclosure Vulnerability         |
| CVE-2020-17029 | Windows Canonical Display Driver Information Disclosure Vulnerability         |
| CVE-2020-17028 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17028 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17027 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17027 | Windows Remote Access Elevation of Privilege Vulnerability                    |
| CVE-2020-17026 | Windows Remote Access Elevation of Privilege Vulnerability                    |

|                |                                                                                   |
|----------------|-----------------------------------------------------------------------------------|
| CVE-2020-17026 | Windows Remote Access Elevation of Privilege Vulnerability                        |
| CVE-2020-17025 | Windows Remote Access Elevation of Privilege Vulnerability                        |
| CVE-2020-17025 | Windows Remote Access Elevation of Privilege Vulnerability                        |
| CVE-2020-17024 | Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability |
| CVE-2020-17024 | Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability |
| CVE-2020-17014 | Windows Print Spooler Elevation of Privilege Vulnerability                        |
| CVE-2020-17014 | Windows Print Spooler Elevation of Privilege Vulnerability                        |
| CVE-2020-17013 | Win32k Information Disclosure Vulnerability                                       |
| CVE-2020-17011 | Windows Port Class Library Elevation of Privilege Vulnerability                   |
| CVE-2020-17011 | Windows Port Class Library Elevation of Privilege Vulnerability                   |
| CVE-2020-17010 | Win32k Elevation of Privilege Vulnerability                                       |
| CVE-2020-17007 | Windows Error Reporting Elevation of Privilege Vulnerability                      |
| CVE-2020-17004 | Windows Graphics Component Information Disclosure Vulnerability                   |
| CVE-2020-17004 | Windows Graphics Component Information Disclosure Vulnerability                   |
| CVE-2020-17001 | Windows Print Spooler Elevation of Privilege Vulnerability                        |
| CVE-2020-17001 | Windows Print Spooler Elevation of Privilege Vulnerability                        |
| CVE-2020-17000 | Remote Desktop Protocol Client Information Disclosure Vulnerability               |
| CVE-2020-17000 | Remote Desktop Protocol Client Information Disclosure Vulnerability               |
| CVE-2020-16999 | Windows WalletService Information Disclosure Vulnerability                        |
| CVE-2020-16998 | DirectX Elevation of Privilege Vulnerability                                      |
| CVE-2020-16997 | Remote Desktop Protocol Server Information Disclosure Vulnerability               |
| CVE-2020-16997 | Remote Desktop Protocol Server Information Disclosure Vulnerability               |
| CVE-2020-16996 | Kerberos Security Feature Bypass Vulnerability                                    |
| CVE-2020-16980 | Windows iSCSI Target Service Elevation of Privilege Vulnerability                 |
| CVE-2020-16976 | Windows Backup Service Elevation of Privilege Vulnerability                       |
| CVE-2020-16975 | Windows Backup Service Elevation of Privilege Vulnerability                       |
| CVE-2020-16974 | Windows Backup Service Elevation of Privilege Vulnerability                       |
| CVE-2020-16973 | Windows Backup Service Elevation of Privilege Vulnerability                       |
| CVE-2020-16972 | Windows Backup Service Elevation of Privilege Vulnerability                       |
| CVE-2020-16968 | Windows Camera Codec Pack Remote Code Execution Vulnerability                     |
| CVE-2020-16967 | Windows Camera Codec Pack Remote Code Execution Vulnerability                     |
| CVE-2020-16964 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16963 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16962 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16961 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16960 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16959 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16958 | Windows Backup Engine Elevation of Privilege Vulnerability                        |
| CVE-2020-16940 | Windows - User Profile Service Elevation of Privilege Vulnerability               |
| CVE-2020-16939 | Group Policy Elevation of Privilege Vulnerability                                 |
| CVE-2020-16938 | Windows Kernel Information Disclosure Vulnerability                               |
| CVE-2020-16937 | .NET Framework Information Disclosure Vulnerability                               |

|                |                                                                                       |
|----------------|---------------------------------------------------------------------------------------|
| CVE-2020-16936 | Windows Backup Service Elevation of Privilege Vulnerability                           |
| CVE-2020-16935 | Windows COM Server Elevation of Privilege Vulnerability                               |
| CVE-2020-16927 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability                 |
| CVE-2020-16924 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-16923 | Microsoft Graphics Components Remote Code Execution Vulnerability                     |
| CVE-2020-16922 | Windows Spoofing Vulnerability                                                        |
| CVE-2020-16921 | Windows Text Services Framework Information Disclosure Vulnerability                  |
| CVE-2020-16920 | Windows Application Compatibility Client Library Elevation of Privilege Vulnerability |
| CVE-2020-16919 | Windows Enterprise App Management Service Information Disclosure Vulnerability        |
| CVE-2020-16916 | Windows COM Server Elevation of Privilege Vulnerability                               |
| CVE-2020-16915 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-16914 | Windows GDI+ Information Disclosure Vulnerability                                     |
| CVE-2020-16913 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-16912 | Windows Backup Service Elevation of Privilege Vulnerability                           |
| CVE-2020-16911 | GDI+ Remote Code Execution Vulnerability                                              |
| CVE-2020-16910 | Windows Security Feature Bypass Vulnerability                                         |
| CVE-2020-16909 | Windows Error Reporting Elevation of Privilege Vulnerability                          |
| CVE-2020-16907 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-16905 | Windows Error Reporting Elevation of Privilege Vulnerability                          |
| CVE-2020-16902 | Windows Installer Elevation of Privilege Vulnerability                                |
| CVE-2020-16900 | Windows Event System Elevation of Privilege Vulnerability                             |
| CVE-2020-16899 | Windows TCP/IP Denial of Service Vulnerability                                        |
| CVE-2020-16898 | Windows TCP/IP Remote Code Execution Vulnerability                                    |
| CVE-2020-16897 | NetBT Information Disclosure Vulnerability                                            |
| CVE-2020-16896 | Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability            |
| CVE-2020-16895 | Windows Error Reporting Manager Elevation of Privilege Vulnerability                  |
| CVE-2020-16894 | Windows NAT Denial of Service Vulnerability                                           |
| CVE-2020-16892 | Windows Image Elevation of Privilege Vulnerability                                    |
| CVE-2020-16891 | Windows Hyper-V Remote Code Execution Vulnerability                                   |
| CVE-2020-16890 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-16889 | Windows KernelStream Information Disclosure Vulnerability                             |
| CVE-2020-16887 | Windows Network Connections Service Elevation of Privilege Vulnerability              |
| CVE-2020-16885 | Windows Storage VSP Driver Elevation of Privilege Vulnerability                       |
| CVE-2020-16879 | Projected Filesystem Information Disclosure Vulnerability                             |
| CVE-2020-16877 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-16876 | Windows Application Compatibility Client Library Elevation of Privilege Vulnerability |
| CVE-2020-16854 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-8927  | Brotli Library Buffer Overflow Vulnerability                                          |
| CVE-2020-1599  | Windows Spoofing Vulnerability                                                        |
| CVE-2020-1599  | Windows Spoofing Vulnerability                                                        |
| CVE-2020-1598  | Windows UPnP Service Elevation of Privilege Vulnerability                             |
| CVE-2020-1596  | TLS Information Disclosure Vulnerability                                              |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-1593 | Windows Media Audio Decoder Remote Code Execution Vulnerability                       |
| CVE-2020-1592 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1590 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-1589 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1587 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability    |
| CVE-2020-1584 | Windows dnssrvr.dll Elevation of Privilege Vulnerability                              |
| CVE-2020-1579 | Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability         |
| CVE-2020-1578 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1577 | DirectWrite Information Disclosure Vulnerability                                      |
| CVE-2020-1570 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-1569 | Microsoft Edge Memory Corruption Vulnerability                                        |
| CVE-2020-1568 | Microsoft Edge PDF Remote Code Execution Vulnerability                                |
| CVE-2020-1567 | MSHTML Engine Remote Code Execution Vulnerability                                     |
| CVE-2020-1566 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1565 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1564 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1562 | Microsoft Graphics Components Remote Code Execution Vulnerability                     |
| CVE-2020-1561 | Microsoft Graphics Components Remote Code Execution Vulnerability                     |
| CVE-2020-1559 | Windows Storage Services Elevation of Privilege Vulnerability                         |
| CVE-2020-1558 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1557 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1556 | Windows WalletService Elevation of Privilege Vulnerability                            |
| CVE-2020-1555 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-1554 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-1553 | Windows Runtime Elevation of Privilege Vulnerability                                  |
| CVE-2020-1552 | Windows Work Folder Service Elevation of Privilege Vulnerability                      |
| CVE-2020-1551 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1550 | Windows CDP User Components Elevation of Privilege Vulnerability                      |
| CVE-2020-1549 | Windows CDP User Components Elevation of Privilege Vulnerability                      |
| CVE-2020-1548 | Windows WaasMedic Service Information Disclosure Vulnerability                        |
| CVE-2020-1547 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1546 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1545 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1544 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1543 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1542 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1541 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1540 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1539 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1538 | Windows UPnP Device Host Elevation of Privilege Vulnerability                         |
| CVE-2020-1537 | Windows Remote Access Elevation of Privilege Vulnerability                            |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-1536 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1535 | Windows Backup Engine Elevation of Privilege Vulnerability                            |
| CVE-2020-1534 | Windows Backup Service Elevation of Privilege Vulnerability                           |
| CVE-2020-1533 | Windows WalletService Elevation of Privilege Vulnerability                            |
| CVE-2020-1532 | Windows InstallService Elevation of Privilege Vulnerability                           |
| CVE-2020-1531 | Windows Accounts Control Elevation of Privilege Vulnerability                         |
| CVE-2020-1530 | Windows Remote Access Elevation of Privilege Vulnerability                            |
| CVE-2020-1529 | Windows GDI Elevation of Privilege Vulnerability                                      |
| CVE-2020-1528 | Windows Radio Manager API Elevation of Privilege Vulnerability                        |
| CVE-2020-1527 | Windows Custom Protocol Engine Elevation of Privilege Vulnerability                   |
| CVE-2020-1526 | Windows Network Connection Broker Elevation of Privilege Vulnerability                |
| CVE-2020-1525 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-1524 | Windows Speech Shell Components Elevation of Privilege Vulnerability                  |
| CVE-2020-1522 | Windows Speech Runtime Elevation of Privilege Vulnerability                           |
| CVE-2020-1521 | Windows Speech Runtime Elevation of Privilege Vulnerability                           |
| CVE-2020-1520 | Windows Font Driver Host Remote Code Execution Vulnerability                          |
| CVE-2020-1519 | Windows UPnP Device Host Elevation of Privilege Vulnerability                         |
| CVE-2020-1518 | Windows File Server Resource Management Service Elevation of Privilege Vulnerability  |
| CVE-2020-1517 | Windows File Server Resource Management Service Elevation of Privilege Vulnerability  |
| CVE-2020-1516 | Windows Work Folders Service Elevation of Privilege Vulnerability                     |
| CVE-2020-1515 | Windows Telephony Server Elevation of Privilege Vulnerability                         |
| CVE-2020-1513 | Windows CSC Service Elevation of Privilege Vulnerability                              |
| CVE-2020-1512 | Windows State Repository Service Information Disclosure Vulnerability                 |
| CVE-2020-1511 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-1510 | Win32k Information Disclosure Vulnerability                                           |
| CVE-2020-1509 | Local Security Authority Subsystem Service Elevation of Privilege Vulnerability       |
| CVE-2020-1508 | Windows Media Audio Decoder Remote Code Execution Vulnerability                       |
| CVE-2020-1507 | Microsoft COM for Windows Elevation of Privilege Vulnerability                        |
| CVE-2020-1506 | Windows Start-Up Application Elevation of Privilege Vulnerability                     |
| CVE-2020-1492 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-1491 | Windows Function Discovery Service Elevation of Privilege Vulnerability               |
| CVE-2020-1490 | Windows Storage Service Elevation of Privilege Vulnerability                          |
| CVE-2020-1489 | Windows CSC Service Elevation of Privilege Vulnerability                              |
| CVE-2020-1488 | Windows AppX Deployment Extensions Elevation of Privilege Vulnerability               |
| CVE-2020-1487 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-1486 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1485 | Windows Image Acquisition Service Information Disclosure Vulnerability                |
| CVE-2020-1484 | Windows Work Folders Service Elevation of Privilege Vulnerability                     |
| CVE-2020-1480 | Windows GDI Elevation of Privilege Vulnerability                                      |
| CVE-2020-1479 | DirectX Elevation of Privilege Vulnerability                                          |

|               |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| CVE-2020-1478 | Media Foundation Memory Corruption Vulnerability                                            |
| CVE-2020-1477 | Media Foundation Memory Corruption Vulnerability                                            |
| CVE-2020-1476 | ASP.NET and .NET Elevation of Privilege Vulnerability                                       |
| CVE-2020-1475 | Windows Server Resource Management Service Elevation of Privilege Vulnerability             |
| CVE-2020-1474 | Windows Image Acquisition Service Information Disclosure Vulnerability                      |
| CVE-2020-1473 | Jet Database Engine Remote Code Execution Vulnerability                                     |
| CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability                                               |
| CVE-2020-1471 | Windows CloudExperienceHost Elevation of Privilege Vulnerability                            |
| CVE-2020-1470 | Windows Work Folders Service Elevation of Privilege Vulnerability                           |
| CVE-2020-1468 | Windows GDI Information Disclosure Vulnerability                                            |
| CVE-2020-1467 | Windows Hard Link Elevation of Privilege Vulnerability                                      |
| CVE-2020-1466 | Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability                 |
| CVE-2020-1464 | Windows Spoofing Vulnerability                                                              |
| CVE-2020-1463 | Windows SharedStream Library Elevation of Privilege Vulnerability                           |
| CVE-2020-1462 | Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability |
| CVE-2020-1459 | Windows ARM Information Disclosure Vulnerability                                            |
| CVE-2020-1441 | Windows Spatial Data Service Elevation of Privilege Vulnerability                           |
| CVE-2020-1438 | Windows Network Connections Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1437 | Windows Network Location Awareness Service Elevation of Privilege Vulnerability             |
| CVE-2020-1436 | Windows Font Library Remote Code Execution Vulnerability                                    |
| CVE-2020-1435 | GDI+ Remote Code Execution Vulnerability                                                    |
| CVE-2020-1434 | Windows Sync Host Service Elevation of Privilege Vulnerability                              |
| CVE-2020-1433 | Microsoft Edge PDF Information Disclosure Vulnerability                                     |
| CVE-2020-1432 | Skype for Business via Internet Explorer Information Disclosure Vulnerability               |
| CVE-2020-1431 | Windows AppX Deployment Extensions Elevation of Privilege Vulnerability                     |
| CVE-2020-1430 | Windows UPnP Device Host Elevation of Privilege Vulnerability                               |
| CVE-2020-1429 | Windows Error Reporting Manager Elevation of Privilege Vulnerability                        |
| CVE-2020-1428 | Windows Network Connections Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1427 | Windows Network Connections Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1426 | Windows Kernel Information Disclosure Vulnerability                                         |
| CVE-2020-1424 | Windows Update Stack Elevation of Privilege Vulnerability                                   |
| CVE-2020-1422 | Windows Runtime Elevation of Privilege Vulnerability                                        |
| CVE-2020-1421 | LNK Remote Code Execution Vulnerability                                                     |
| CVE-2020-1420 | Windows Error Reporting Information Disclosure Vulnerability                                |
| CVE-2020-1419 | Windows Kernel Information Disclosure Vulnerability                                         |
| CVE-2020-1418 | Windows Diagnostics Hub Elevation of Privilege Vulnerability                                |
| CVE-2020-1417 | Windows Kernel Elevation of Privilege Vulnerability                                         |
| CVE-2020-1415 | Windows Runtime Elevation of Privilege Vulnerability                                        |
| CVE-2020-1414 | Windows Runtime Elevation of Privilege Vulnerability                                        |
| CVE-2020-1413 | Windows Runtime Elevation of Privilege Vulnerability                                        |
| CVE-2020-1412 | Microsoft Graphics Components Remote Code Execution Vulnerability                           |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-1411 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1410 | Windows Address Book Remote Code Execution Vulnerability                              |
| CVE-2020-1409 | DirectWrite Remote Code Execution Vulnerability                                       |
| CVE-2020-1408 | Microsoft Graphics Remote Code Execution Vulnerability                                |
| CVE-2020-1407 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1406 | Windows Network List Service Elevation of Privilege Vulnerability                     |
| CVE-2020-1405 | Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability     |
| CVE-2020-1404 | Windows Runtime Elevation of Privilege Vulnerability                                  |
| CVE-2020-1403 | VBScript Remote Code Execution Vulnerability                                          |
| CVE-2020-1402 | Windows ActiveX Installer Service Elevation of Privilege Vulnerability                |
| CVE-2020-1401 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1400 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1399 | Windows Runtime Elevation of Privilege Vulnerability                                  |
| CVE-2020-1398 | Windows Lockscreen Elevation of Privilege Vulnerability                               |
| CVE-2020-1397 | Windows Imaging Component Information Disclosure Vulnerability                        |
| CVE-2020-1396 | Windows ALPC Elevation of Privilege Vulnerability                                     |
| CVE-2020-1395 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1394 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1393 | Windows Diagnostics Hub Elevation of Privilege Vulnerability                          |
| CVE-2020-1392 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1391 | Windows Agent Activation Runtime Information Disclosure Vulnerability                 |
| CVE-2020-1390 | Windows Network Connections Service Elevation of Privilege Vulnerability              |
| CVE-2020-1389 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1388 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1387 | Windows Push Notification Service Elevation of Privilege Vulnerability                |
| CVE-2020-1386 | Connected User Experiences and Telemetry Service Information Disclosure Vulnerability |
| CVE-2020-1385 | Windows Credential Picker Elevation of Privilege Vulnerability                        |
| CVE-2020-1384 | Windows CNG Key Isolation Service Elevation of Privilege Vulnerability                |
| CVE-2020-1383 | Windows RRAS Service Information Disclosure Vulnerability                             |
| CVE-2020-1382 | Windows Graphics Component Elevation of Privilege Vulnerability                       |
| CVE-2020-1381 | Windows Graphics Component Elevation of Privilege Vulnerability                       |
| CVE-2020-1380 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-1379 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-1378 | Windows Registry Elevation of Privilege Vulnerability                                 |
| CVE-2020-1377 | Windows Registry Elevation of Privilege Vulnerability                                 |
| CVE-2020-1376 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1375 | Windows COM Server Elevation of Privilege Vulnerability                               |
| CVE-2020-1374 | Remote Desktop Client Remote Code Execution Vulnerability                             |
| CVE-2020-1373 | Windows Network Connections Service Elevation of Privilege Vulnerability              |
| CVE-2020-1372 | Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability     |
| CVE-2020-1371 | Windows Event Logging Service Elevation of Privilege Vulnerability                    |

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

|               |                                                                            |
|---------------|----------------------------------------------------------------------------|
| CVE-2020-1308 | DirectX Elevation of Privilege Vulnerability                               |
| CVE-2020-1307 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1306 | Windows Runtime Elevation of Privilege Vulnerability                       |
| CVE-2020-1305 | Windows State Repository Service Elevation of Privilege Vulnerability      |
| CVE-2020-1304 | Windows Runtime Elevation of Privilege Vulnerability                       |
| CVE-2020-1303 | Windows Runtime Elevation of Privilege Vulnerability                       |
| CVE-2020-1302 | Windows Installer Elevation of Privilege Vulnerability                     |
| CVE-2020-1301 | Windows SMB Authenticated Remote Code Execution Vulnerability              |
| CVE-2020-1300 | Windows Remote Code Execution Vulnerability                                |
| CVE-2020-1299 | LNK Remote Code Execution Vulnerability                                    |
| CVE-2020-1296 | Windows Diagnostics & feedback Information Disclosure Vulnerability        |
| CVE-2020-1294 | Windows WalletService Elevation of Privilege Vulnerability                 |
| CVE-2020-1293 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability    |
| CVE-2020-1292 | OpenSSH for Windows Elevation of Privilege Vulnerability                   |
| CVE-2020-1291 | Windows Network Connections Service Elevation of Privilege Vulnerability   |
| CVE-2020-1290 | Win32k Information Disclosure Vulnerability                                |
| CVE-2020-1287 | Windows WalletService Elevation of Privilege Vulnerability                 |
| CVE-2020-1286 | Windows Shell Remote Code Execution Vulnerability                          |
| CVE-2020-1285 | GDI+ Remote Code Execution Vulnerability                                   |
| CVE-2020-1283 | Windows Denial of Service Vulnerability                                    |
| CVE-2020-1282 | Windows Runtime Elevation of Privilege Vulnerability                       |
| CVE-2020-1281 | Windows OLE Remote Code Execution Vulnerability                            |
| CVE-2020-1280 | Windows Bluetooth Service Elevation of Privilege Vulnerability             |
| CVE-2020-1279 | Windows Lockscreen Elevation of Privilege Vulnerability                    |
| CVE-2020-1278 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability    |
| CVE-2020-1277 | Windows Installer Elevation of Privilege Vulnerability                     |
| CVE-2020-1276 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1275 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1274 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1273 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1272 | Windows Installer Elevation of Privilege Vulnerability                     |
| CVE-2020-1271 | Windows Backup Service Elevation of Privilege Vulnerability                |
| CVE-2020-1270 | Windows WLAN Service Elevation of Privilege Vulnerability                  |
| CVE-2020-1269 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1268 | Windows Service Information Disclosure Vulnerability                       |
| CVE-2020-1267 | Local Security Authority Subsystem Service Denial of Service Vulnerability |
| CVE-2020-1266 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1265 | Windows Runtime Elevation of Privilege Vulnerability                       |
| CVE-2020-1264 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1263 | Windows Error Reporting Information Disclosure Vulnerability               |
| CVE-2020-1262 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-1261 | Windows Error Reporting Information Disclosure Vulnerability               |

|               |                                                                                      |
|---------------|--------------------------------------------------------------------------------------|
| CVE-2020-1260 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1259 | Windows Host Guardian Service Security Feature Bypass Vulnerability                  |
| CVE-2020-1258 | DirectX Elevation of Privilege Vulnerability                                         |
| CVE-2020-1257 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability              |
| CVE-2020-1256 | Windows GDI Information Disclosure Vulnerability                                     |
| CVE-2020-1255 | Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability |
| CVE-2020-1254 | Windows Modules Installer Service Elevation of Privilege Vulnerability               |
| CVE-2020-1253 | Win32k Elevation of Privilege Vulnerability                                          |
| CVE-2020-1252 | Windows Remote Code Execution Vulnerability                                          |
| CVE-2020-1251 | Win32k Elevation of Privilege Vulnerability                                          |
| CVE-2020-1250 | Win32k Information Disclosure Vulnerability                                          |
| CVE-2020-1249 | Windows Runtime Elevation of Privilege Vulnerability                                 |
| CVE-2020-1248 | GDI+ Remote Code Execution Vulnerability                                             |
| CVE-2020-1247 | Win32k Elevation of Privilege Vulnerability                                          |
| CVE-2020-1246 | Windows Kernel Elevation of Privilege Vulnerability                                  |
| CVE-2020-1245 | Win32k Elevation of Privilege Vulnerability                                          |
| CVE-2020-1244 | Connected User Experiences and Telemetry Service Denial of Service Vulnerability     |
| CVE-2020-1243 | Windows Hyper-V Denial of Service Vulnerability                                      |
| CVE-2020-1242 | Microsoft Edge Information Disclosure Vulnerability                                  |
| CVE-2020-1241 | Windows Kernel Security Feature Bypass Vulnerability                                 |
| CVE-2020-1239 | Media Foundation Memory Corruption Vulnerability                                     |
| CVE-2020-1238 | Media Foundation Memory Corruption Vulnerability                                     |
| CVE-2020-1237 | Windows Kernel Elevation of Privilege Vulnerability                                  |
| CVE-2020-1236 | Jet Database Engine Remote Code Execution Vulnerability                              |
| CVE-2020-1235 | Windows Runtime Elevation of Privilege Vulnerability                                 |
| CVE-2020-1234 | Windows Error Reporting Elevation of Privilege Vulnerability                         |
| CVE-2020-1233 | Windows Runtime Elevation of Privilege Vulnerability                                 |
| CVE-2020-1232 | Media Foundation Information Disclosure Vulnerability                                |
| CVE-2020-1231 | Windows Runtime Elevation of Privilege Vulnerability                                 |
| CVE-2020-1230 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1228 | Windows DNS Denial of Service Vulnerability                                          |
| CVE-2020-1222 | Microsoft Store Runtime Elevation of Privilege Vulnerability                         |
| CVE-2020-1220 | Microsoft Edge (Chromium-based) in IE Mode Spoofing Vulnerability                    |
| CVE-2020-1219 | Microsoft Browser Memory Corruption Vulnerability                                    |
| CVE-2020-1217 | Windows Runtime Information Disclosure Vulnerability                                 |
| CVE-2020-1216 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1215 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1214 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1213 | VBScript Remote Code Execution Vulnerability                                         |
| CVE-2020-1212 | OLE Automation Elevation of Privilege Vulnerability                                  |
| CVE-2020-1211 | Connected Devices Platform Service Elevation of Privilege Vulnerability              |
| CVE-2020-1209 | Windows Network List Service Elevation of Privilege Vulnerability                    |

|               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| CVE-2020-1208 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1207 | Win32k Elevation of Privilege Vulnerability                                       |
| CVE-2020-1206 | Windows SMBv3 Client/Server Information Disclosure Vulnerability                  |
| CVE-2020-1204 | Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability |
| CVE-2020-1203 | Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability            |
| CVE-2020-1202 | Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability            |
| CVE-2020-1201 | Windows Now Playing Session Manager Elevation of Privilege Vulnerability          |
| CVE-2020-1199 | Windows Feedback Hub Elevation of Privilege Vulnerability                         |
| CVE-2020-1197 | Windows Error Reporting Manager Elevation of Privilege Vulnerability              |
| CVE-2020-1196 | Windows Print Configuration Elevation of Privilege Vulnerability                  |
| CVE-2020-1194 | Windows Registry Denial of Service Vulnerability                                  |
| CVE-2020-1191 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1190 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1189 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1188 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1187 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1186 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1185 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1184 | Windows State Repository Service Elevation of Privilege Vulnerability             |
| CVE-2020-1180 | Scripting Engine Memory Corruption Vulnerability                                  |
| CVE-2020-1179 | Windows GDI Information Disclosure Vulnerability                                  |
| CVE-2020-1176 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1175 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1174 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1172 | Scripting Engine Memory Corruption Vulnerability                                  |
| CVE-2020-1169 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1167 | Microsoft Graphics Components Remote Code Execution Vulnerability                 |
| CVE-2020-1166 | Windows Clipboard Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1165 | Windows Clipboard Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1164 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1162 | Windows Elevation of Privilege Vulnerability                                      |
| CVE-2020-1160 | Microsoft Graphics Component Information Disclosure Vulnerability                 |
| CVE-2020-1159 | Windows Elevation of Privilege Vulnerability                                      |
| CVE-2020-1158 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1157 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1156 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1155 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1154 | Windows Common Log File System Driver Elevation of Privilege Vulnerability        |
| CVE-2020-1153 | Microsoft Graphics Components Remote Code Execution Vulnerability                 |
| CVE-2020-1152 | Windows Win32k Elevation of Privilege Vulnerability                               |
| CVE-2020-1151 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1149 | Windows Runtime Elevation of Privilege Vulnerability                              |

|               |                                                                                          |
|---------------|------------------------------------------------------------------------------------------|
| CVE-2020-1147 | .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability |
| CVE-2020-1147 | .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability |
| CVE-2020-1146 | Microsoft Store Runtime Elevation of Privilege Vulnerability                             |
| CVE-2020-1145 | Windows GDI Information Disclosure Vulnerability                                         |
| CVE-2020-1144 | Windows State Repository Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1143 | Win32k Elevation of Privilege Vulnerability                                              |
| CVE-2020-1142 | Windows GDI Elevation of Privilege Vulnerability                                         |
| CVE-2020-1141 | Windows GDI Information Disclosure Vulnerability                                         |
| CVE-2020-1140 | DirectX Elevation of Privilege Vulnerability                                             |
| CVE-2020-1139 | Windows Runtime Elevation of Privilege Vulnerability                                     |
| CVE-2020-1138 | Windows Storage Service Elevation of Privilege Vulnerability                             |
| CVE-2020-1137 | Windows Push Notification Service Elevation of Privilege Vulnerability                   |
| CVE-2020-1136 | Media Foundation Memory Corruption Vulnerability                                         |
| CVE-2020-1135 | Windows Graphics Component Elevation of Privilege Vulnerability                          |
| CVE-2020-1134 | Windows State Repository Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1133 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability                  |
| CVE-2020-1132 | Windows Error Reporting Manager Elevation of Privilege Vulnerability                     |
| CVE-2020-1131 | Windows State Repository Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1130 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability                  |
| CVE-2020-1129 | Microsoft Windows Codecs Library Remote Code Execution Vulnerability                     |
| CVE-2020-1126 | Media Foundation Memory Corruption Vulnerability                                         |
| CVE-2020-1125 | Windows Runtime Elevation of Privilege Vulnerability                                     |
| CVE-2020-1124 | Windows State Repository Service Elevation of Privilege Vulnerability                    |
| CVE-2020-1123 | Connected User Experiences and Telemetry Service Denial of Service Vulnerability         |
| CVE-2020-1122 | Windows Language Pack Installer Elevation of Privilege Vulnerability                     |
| CVE-2020-1121 | Windows Clipboard Service Elevation of Privilege Vulnerability                           |
| CVE-2020-1119 | Windows Information Disclosure Vulnerability                                             |
| CVE-2020-1118 | Microsoft Windows Transport Layer Security Denial of Service Vulnerability               |
| CVE-2020-1117 | Microsoft Color Management Remote Code Execution Vulnerability                           |
| CVE-2020-1116 | Windows CSRSS Information Disclosure Vulnerability                                       |
| CVE-2020-1115 | Windows Common Log File System Driver Elevation of Privilege Vulnerability               |
| CVE-2020-1114 | Windows Kernel Elevation of Privilege Vulnerability                                      |
| CVE-2020-1113 | Windows Task Scheduler Security Feature Bypass Vulnerability                             |
| CVE-2020-1112 | Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability     |
| CVE-2020-1111 | Windows Clipboard Service Elevation of Privilege Vulnerability                           |
| CVE-2020-1110 | Windows Update Stack Elevation of Privilege Vulnerability                                |
| CVE-2020-1109 | Windows Update Stack Elevation of Privilege Vulnerability                                |
| CVE-2020-1108 | .NET Core & .NET Framework Denial of Service Vulnerability                               |
| CVE-2020-1098 | Windows Shell Infrastructure Component Elevation of Privilege Vulnerability              |
| CVE-2020-1097 | Windows Graphics Component Information Disclosure Vulnerability                          |

|               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| CVE-2020-1096 | Microsoft Edge PDF Remote Code Execution Vulnerability                            |
| CVE-2020-1094 | Windows Work Folder Service Elevation of Privilege Vulnerability                  |
| CVE-2020-1093 | VBScript Remote Code Execution Vulnerability                                      |
| CVE-2020-1092 | Internet Explorer Memory Corruption Vulnerability                                 |
| CVE-2020-1091 | Windows Graphics Component Information Disclosure Vulnerability                   |
| CVE-2020-1090 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1088 | Windows Error Reporting Elevation of Privilege Vulnerability                      |
| CVE-2020-1087 | Windows Kernel Elevation of Privilege Vulnerability                               |
| CVE-2020-1086 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1085 | Windows Function Discovery Service Elevation of Privilege Vulnerability           |
| CVE-2020-1084 | Connected User Experiences and Telemetry Service Denial of Service Vulnerability  |
| CVE-2020-1083 | Microsoft Graphics Component Information Disclosure Vulnerability                 |
| CVE-2020-1082 | Windows Error Reporting Elevation of Privilege Vulnerability                      |
| CVE-2020-1081 | Windows Printer Service Elevation of Privilege Vulnerability                      |
| CVE-2020-1080 | Windows Hyper-V Elevation of Privilege Vulnerability                              |
| CVE-2020-1079 | Microsoft Windows Elevation of Privilege Vulnerability                            |
| CVE-2020-1078 | Windows Installer Elevation of Privilege Vulnerability                            |
| CVE-2020-1077 | Windows Runtime Elevation of Privilege Vulnerability                              |
| CVE-2020-1076 | Windows Denial of Service Vulnerability                                           |
| CVE-2020-1075 | Windows Subsystem for Linux Information Disclosure Vulnerability                  |
| CVE-2020-1074 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1073 | Scripting Engine Memory Corruption Vulnerability                                  |
| CVE-2020-1072 | Windows Kernel Information Disclosure Vulnerability                               |
| CVE-2020-1071 | Windows Remote Access Common Dialog Elevation of Privilege Vulnerability          |
| CVE-2020-1070 | Windows Print Spooler Elevation of Privilege Vulnerability                        |
| CVE-2020-1068 | Microsoft Windows Elevation of Privilege Vulnerability                            |
| CVE-2020-1067 | Windows Remote Code Execution Vulnerability                                       |
| CVE-2020-1065 | Scripting Engine Memory Corruption Vulnerability                                  |
| CVE-2020-1064 | MSHTML Engine Remote Code Execution Vulnerability                                 |
| CVE-2020-1062 | Internet Explorer Memory Corruption Vulnerability                                 |
| CVE-2020-1061 | Microsoft Script Runtime Remote Code Execution Vulnerability                      |
| CVE-2020-1060 | VBScript Remote Code Execution Vulnerability                                      |
| CVE-2020-1059 | Microsoft Edge Spoofing Vulnerability                                             |
| CVE-2020-1058 | VBScript Remote Code Execution Vulnerability                                      |
| CVE-2020-1057 | Scripting Engine Memory Corruption Vulnerability                                  |
| CVE-2020-1056 | Microsoft Edge Elevation of Privilege Vulnerability                               |
| CVE-2020-1055 | Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability |
| CVE-2020-1054 | Win32k Elevation of Privilege Vulnerability                                       |
| CVE-2020-1053 | DirectX Elevation of Privilege Vulnerability                                      |
| CVE-2020-1052 | Windows Elevation of Privilege Vulnerability                                      |
| CVE-2020-1051 | Jet Database Engine Remote Code Execution Vulnerability                           |
| CVE-2020-1048 | Windows Print Spooler Elevation of Privilege Vulnerability                        |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-1047 | Windows Hyper-V Elevation of Privilege Vulnerability                                  |
| CVE-2020-1046 | .NET Framework Remote Code Execution Vulnerability                                    |
| CVE-2020-1039 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1038 | Windows Routing Utilities Denial of Service                                           |
| CVE-2020-1037 | Chakra Scripting Engine Memory Corruption Vulnerability                               |
| CVE-2020-1035 | VBScript Remote Code Execution Vulnerability                                          |
| CVE-2020-1034 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1033 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1031 | Windows DHCP Server Information Disclosure Vulnerability                              |
| CVE-2020-1030 | Windows Print Spooler Elevation of Privilege Vulnerability                            |
| CVE-2020-1029 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-1028 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-1027 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1021 | Windows Error Reporting Elevation of Privilege Vulnerability                          |
| CVE-2020-1020 | Adobe Font Manager Library Remote Code Execution Vulnerability                        |
| CVE-2020-1017 | Windows Push Notification Service Elevation of Privilege Vulnerability                |
| CVE-2020-1016 | Windows Push Notification Service Information Disclosure Vulnerability                |
| CVE-2020-1015 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1014 | Microsoft Windows Update Client Elevation of Privilege Vulnerability                  |
| CVE-2020-1013 | Group Policy Elevation of Privilege Vulnerability                                     |
| CVE-2020-1012 | WinINet API Elevation of Privilege Vulnerability                                      |
| CVE-2020-1011 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1010 | Microsoft Windows Elevation of Privilege Vulnerability                                |
| CVE-2020-1009 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-1008 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-1007 | Windows Kernel Information Disclosure Vulnerability                                   |
| CVE-2020-1006 | Windows Push Notification Service Elevation of Privilege Vulnerability                |
| CVE-2020-1005 | Microsoft Graphics Component Information Disclosure Vulnerability                     |
| CVE-2020-1004 | Windows Graphics Component Elevation of Privilege Vulnerability                       |
| CVE-2020-1003 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-1001 | Windows Push Notification Service Elevation of Privilege Vulnerability                |
| CVE-2020-1000 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-0999 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0998 | Windows Graphics Component Elevation of Privilege Vulnerability                       |
| CVE-2020-0997 | Windows Camera Codec Pack Remote Code Execution Vulnerability                         |
| CVE-2020-0996 | Windows Update Stack Elevation of Privilege Vulnerability                             |
| CVE-2020-0995 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0994 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0993 | Windows DNS Denial of Service Vulnerability                                           |
| CVE-2020-0992 | Jet Database Engine Remote Code Execution Vulnerability                               |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-0989 | Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability     |
| CVE-2020-0988 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0987 | Microsoft Graphics Component Information Disclosure Vulnerability                     |
| CVE-2020-0986 | Windows Kernel Elevation of Privilege Vulnerability                                   |
| CVE-2020-0985 | Windows Update Stack Elevation of Privilege Vulnerability                             |
| CVE-2020-0983 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-0982 | Microsoft Graphics Component Information Disclosure Vulnerability                     |
| CVE-2020-0981 | Windows Token Security Feature Bypass Vulnerability                                   |
| CVE-2020-0970 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-0969 | Chakra Scripting Engine Memory Corruption Vulnerability                               |
| CVE-2020-0968 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-0967 | VBScript Remote Code Execution Vulnerability                                          |
| CVE-2020-0966 | VBScript Remote Code Execution Vulnerability                                          |
| CVE-2020-0965 | Microsoft Windows Codecs Library Remote Code Execution Vulnerability                  |
| CVE-2020-0964 | GDI+ Remote Code Execution Vulnerability                                              |
| CVE-2020-0963 | Windows GDI Information Disclosure Vulnerability                                      |
| CVE-2020-0962 | Win32k Information Disclosure Vulnerability                                           |
| CVE-2020-0960 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0959 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0958 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-0956 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-0955 | Windows Kernel Information Disclosure in CPU Memory Access                            |
| CVE-2020-0953 | Jet Database Engine Remote Code Execution Vulnerability                               |
| CVE-2020-0952 | Windows GDI Information Disclosure Vulnerability                                      |
| CVE-2020-0951 | Windows Defender Application Control Security Feature Bypass Vulnerability            |
| CVE-2020-0950 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-0949 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-0948 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-0947 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-0946 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-0945 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-0944 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-0942 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-0941 | Win32k Information Disclosure Vulnerability                                           |
| CVE-2020-0940 | Windows Push Notification Service Elevation of Privilege Vulnerability                |
| CVE-2020-0939 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-0938 | Adobe Font Manager Library Remote Code Execution Vulnerability                        |
| CVE-2020-0937 | Media Foundation Information Disclosure Vulnerability                                 |
| CVE-2020-0936 | Windows Scheduled Task Elevation of Privilege Vulnerability                           |
| CVE-2020-0934 | Windows Elevation of Privilege Vulnerability                                          |

|               |                                                                               |
|---------------|-------------------------------------------------------------------------------|
| CVE-2020-0928 | Windows Kernel Information Disclosure Vulnerability                           |
| CVE-2020-0922 | Microsoft COM for Windows Remote Code Execution Vulnerability                 |
| CVE-2020-0921 | Microsoft Graphics Component Information Disclosure Vulnerability             |
| CVE-2020-0918 | Windows Hyper-V Elevation of Privilege Vulnerability                          |
| CVE-2020-0917 | Windows Hyper-V Elevation of Privilege Vulnerability                          |
| CVE-2020-0916 | Windows GDI Elevation of Privilege Vulnerability                              |
| CVE-2020-0915 | Windows GDI Elevation of Privilege Vulnerability                              |
| CVE-2020-0914 | Windows State Repository Service Information Disclosure Vulnerability         |
| CVE-2020-0913 | Windows Kernel Elevation of Privilege Vulnerability                           |
| CVE-2020-0912 | Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability |
| CVE-2020-0911 | Windows Modules Installer Elevation of Privilege Vulnerability                |
| CVE-2020-0910 | Windows Hyper-V Remote Code Execution Vulnerability                           |
| CVE-2020-0909 | Windows Hyper-V Denial of Service Vulnerability                               |
| CVE-2020-0908 | Windows Text Service Module Remote Code Execution Vulnerability               |
| CVE-2020-0907 | Microsoft Graphics Components Remote Code Execution Vulnerability             |
| CVE-2020-0904 | Windows Hyper-V Denial of Service Vulnerability                               |
| CVE-2020-0897 | Windows Work Folder Service Elevation of Privilege Vulnerability              |
| CVE-2020-0896 | Windows Hard Link Elevation of Privilege Vulnerability                        |
| CVE-2020-0895 | Windows VBScript Engine Remote Code Execution Vulnerability                   |
| CVE-2020-0890 | Windows Hyper-V Denial of Service Vulnerability                               |
| CVE-2020-0889 | Jet Database Engine Remote Code Execution Vulnerability                       |
| CVE-2020-0888 | DirectX Elevation of Privilege Vulnerability                                  |
| CVE-2020-0887 | Win32k Elevation of Privilege Vulnerability                                   |
| CVE-2020-0886 | Windows Storage Services Elevation of Privilege Vulnerability                 |
| CVE-2020-0885 | Windows Graphics Component Information Disclosure Vulnerability               |
| CVE-2020-0883 | GDI+ Remote Code Execution Vulnerability                                      |
| CVE-2020-0882 | Windows GDI Information Disclosure Vulnerability                              |
| CVE-2020-0881 | GDI+ Remote Code Execution Vulnerability                                      |
| CVE-2020-0880 | Windows GDI Information Disclosure Vulnerability                              |
| CVE-2020-0879 | Windows GDI Information Disclosure Vulnerability                              |
| CVE-2020-0878 | Microsoft Browser Memory Corruption Vulnerability                             |
| CVE-2020-0877 | Win32k Elevation of Privilege Vulnerability                                   |
| CVE-2020-0876 | Win32k Information Disclosure Vulnerability                                   |
| CVE-2020-0875 | Microsoft splwow64 Information Disclosure Vulnerability                       |
| CVE-2020-0874 | Windows GDI Information Disclosure Vulnerability                              |
| CVE-2020-0871 | Windows Network Connections Service Information Disclosure Vulnerability      |
| CVE-2020-0870 | Shell infrastructure component Elevation of Privilege Vulnerability           |
| CVE-2020-0869 | Media Foundation Memory Corruption Vulnerability                              |
| CVE-2020-0868 | Windows Update Orchestrator Service Elevation of Privilege Vulnerability      |
| CVE-2020-0867 | Windows Update Orchestrator Service Elevation of Privilege Vulnerability      |
| CVE-2020-0866 | Windows Work Folder Service Elevation of Privilege Vulnerability              |
| CVE-2020-0865 | Windows Work Folder Service Elevation of Privilege Vulnerability              |

|               |                                                                                            |
|---------------|--------------------------------------------------------------------------------------------|
| CVE-2020-0864 | Windows Work Folder Service Elevation of Privilege Vulnerability                           |
| CVE-2020-0863 | Connected User Experiences and Telemetry Service Information Disclosure Vulnerability      |
| CVE-2020-0861 | Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability |
| CVE-2020-0860 | Windows ActiveX Installer Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0859 | Windows Modules Installer Service Information Disclosure Vulnerability                     |
| CVE-2020-0858 | Windows Elevation of Privilege Vulnerability                                               |
| CVE-2020-0857 | Windows Search Indexer Elevation of Privilege Vulnerability                                |
| CVE-2020-0856 | Active Directory Information Disclosure Vulnerability                                      |
| CVE-2020-0854 | Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability          |
| CVE-2020-0853 | CVE-2020-0853   Windows Imaging Component Information Disclosure Vulnerability             |
| CVE-2020-0849 | CVE-2020-0849   Windows Hard Link Elevation of Privilege Vulnerability                     |
| CVE-2020-0848 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0847 | VBScript Remote Code Execution Vulnerability                                               |
| CVE-2020-0845 | Windows Network Connections Service Elevation of Privilege Vulnerability                   |
| CVE-2020-0844 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability      |
| CVE-2020-0843 | Windows Installer Elevation of Privilege Vulnerability                                     |
| CVE-2020-0842 | Windows Installer Elevation of Privilege Vulnerability                                     |
| CVE-2020-0841 | Windows Hard Link Elevation of Privilege Vulnerability                                     |
| CVE-2020-0840 | Windows Hard Link Elevation of Privilege Vulnerability                                     |
| CVE-2020-0839 | Windows dnssrvr.dll Elevation of Privilege Vulnerability                                   |
| CVE-2020-0838 | NTFS Elevation of Privilege Vulnerability                                                  |
| CVE-2020-0837 | ADFS Spoofing Vulnerability                                                                |
| CVE-2020-0836 | Windows DNS Denial of Service Vulnerability                                                |
| CVE-2020-0834 | Windows ALPC Elevation of Privilege Vulnerability                                          |
| CVE-2020-0833 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0832 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0831 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0830 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0829 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0828 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0827 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0826 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0825 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0824 | Internet Explorer Memory Corruption Vulnerability                                          |
| CVE-2020-0823 | Scripting Engine Memory Corruption Vulnerability                                           |
| CVE-2020-0822 | Windows Language Pack Installer Elevation of Privilege Vulnerability                       |
| CVE-2020-0821 | Windows Kernel Information Disclosure Vulnerability                                        |
| CVE-2020-0820 | Media Foundation Information Disclosure Vulnerability                                      |
| CVE-2020-0819 | Windows Device Setup Manager Elevation of Privilege Vulnerability                          |
| CVE-2020-0818 | Windows Elevation of Privilege Vulnerability                                               |

|               |                                                                                      |
|---------------|--------------------------------------------------------------------------------------|
| CVE-2020-0817 | Remote Desktop Client Remote Code Execution Vulnerability                            |
| CVE-2020-0816 | Microsoft Edge Memory Corruption Vulnerability                                       |
| CVE-2020-0814 | Windows Installer Elevation of Privilege Vulnerability                               |
| CVE-2020-0813 | Scripting Engine Information Disclosure Vulnerability                                |
| CVE-2020-0812 | Chakra Scripting Engine Memory Corruption Vulnerability                              |
| CVE-2020-0811 | Chakra Scripting Engine Memory Corruption Vulnerability                              |
| CVE-2020-0810 | Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability               |
| CVE-2020-0809 | Media Foundation Memory Corruption Vulnerability                                     |
| CVE-2020-0808 | Provisioning Runtime Elevation of Privilege Vulnerability                            |
| CVE-2020-0807 | Media Foundation Memory Corruption Vulnerability                                     |
| CVE-2020-0806 | Windows Error Reporting Elevation of Privilege Vulnerability                         |
| CVE-2020-0805 | Projected Filesystem Security Feature Bypass Vulnerability                           |
| CVE-2020-0804 | Windows Network Connections Service Elevation of Privilege Vulnerability             |
| CVE-2020-0803 | Windows Network Connections Service Elevation of Privilege Vulnerability             |
| CVE-2020-0802 | Windows Network Connections Service Elevation of Privilege Vulnerability             |
| CVE-2020-0801 | Media Foundation Memory Corruption Vulnerability                                     |
| CVE-2020-0800 | Windows Work Folder Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0799 | Windows Kernel Elevation of Privilege Vulnerability                                  |
| CVE-2020-0798 | Windows Installer Elevation of Privilege Vulnerability                               |
| CVE-2020-0797 | Windows Work Folder Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0796 | Windows SMBv3 Client/Server Remote Code Execution Vulnerability                      |
| CVE-2020-0794 | Windows Denial of Service Vulnerability                                              |
| CVE-2020-0793 | Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability              |
| CVE-2020-0792 | Windows Graphics Component Elevation of Privilege Vulnerability                      |
| CVE-2020-0791 | Windows Graphics Component Elevation of Privilege Vulnerability                      |
| CVE-2020-0790 | Microsoft splwow64 Elevation of Privilege Vulnerability                              |
| CVE-2020-0788 | Win32k Elevation of Privilege Vulnerability                                          |
| CVE-2020-0787 | Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability |
| CVE-2020-0785 | Windows User Profile Service Elevation of Privilege Vulnerability                    |
| CVE-2020-0784 | DirectX Elevation of Privilege Vulnerability                                         |
| CVE-2020-0783 | Windows UPnP Service Elevation of Privilege Vulnerability                            |
| CVE-2020-0782 | Windows Cryptographic Catalog Services Elevation of Privilege Vulnerability          |
| CVE-2020-0781 | Windows UPnP Service Elevation of Privilege Vulnerability                            |
| CVE-2020-0780 | Windows Network List Service Elevation of Privilege Vulnerability                    |
| CVE-2020-0779 | Windows Installer Elevation of Privilege Vulnerability                               |
| CVE-2020-0778 | Windows Network Connections Service Elevation of Privilege Vulnerability             |
| CVE-2020-0777 | Windows Work Folder Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0776 | Windows Elevation of Privilege Vulnerability                                         |
| CVE-2020-0775 | Windows Error Reporting Information Disclosure Vulnerability                         |
| CVE-2020-0774 | Windows GDI Information Disclosure Vulnerability                                     |
| CVE-2020-0773 | Windows ActiveX Installer Service Elevation of Privilege Vulnerability               |
| CVE-2020-0772 | Windows Error Reporting Elevation of Privilege Vulnerability                         |

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| CVE-2020-0771 | Windows CSC Service Elevation of Privilege Vulnerability                              |
| CVE-2020-0770 | Windows ActiveX Installer Service Elevation of Privilege Vulnerability                |
| CVE-2020-0769 | Windows CSC Service Elevation of Privilege Vulnerability                              |
| CVE-2020-0768 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-0767 | Scripting Engine Memory Corruption Vulnerability                                      |
| CVE-2020-0766 | Microsoft Store Runtime Elevation of Privilege Vulnerability                          |
| CVE-2020-0764 | Windows Storage Services Elevation of Privilege Vulnerability                         |
| CVE-2020-0763 | Windows Defender Security Center Elevation of Privilege Vulnerability                 |
| CVE-2020-0762 | Windows Defender Security Center Elevation of Privilege Vulnerability                 |
| CVE-2020-0761 | Active Directory Remote Code Execution Vulnerability                                  |
| CVE-2020-0757 | Windows SSH Elevation of Privilege Vulnerability                                      |
| CVE-2020-0756 | Windows Key Isolation Service Information Disclosure Vulnerability                    |
| CVE-2020-0755 | Windows Key Isolation Service Information Disclosure Vulnerability                    |
| CVE-2020-0754 | Windows Error Reporting Elevation of Privilege Vulnerability                          |
| CVE-2020-0753 | Windows Error Reporting Elevation of Privilege Vulnerability                          |
| CVE-2020-0752 | Windows Search Indexer Elevation of Privilege Vulnerability                           |
| CVE-2020-0751 | Windows Hyper-V Denial of Service Vulnerability                                       |
| CVE-2020-0750 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0749 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0748 | Windows Key Isolation Service Information Disclosure Vulnerability                    |
| CVE-2020-0747 | Windows Data Sharing Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0746 | Microsoft Graphics Components Information Disclosure Vulnerability                    |
| CVE-2020-0745 | Windows Graphics Component Elevation of Privilege Vulnerability                       |
| CVE-2020-0744 | Windows GDI Information Disclosure Vulnerability                                      |
| CVE-2020-0743 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0742 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0741 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0740 | Connected Devices Platform Service Elevation of Privilege Vulnerability               |
| CVE-2020-0739 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-0738 | Media Foundation Memory Corruption Vulnerability                                      |
| CVE-2020-0737 | Windows Elevation of Privilege Vulnerability                                          |
| CVE-2020-0735 | Windows Search Indexer Elevation of Privilege Vulnerability                           |
| CVE-2020-0734 | Remote Desktop Client Remote Code Execution Vulnerability                             |
| CVE-2020-0731 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-0730 | Windows User Profile Service Elevation of Privilege Vulnerability                     |
| CVE-2020-0729 | LNK Remote Code Execution Vulnerability                                               |
| CVE-2020-0728 | Windows Modules Installer Service Information Disclosure Vulnerability                |
| CVE-2020-0727 | Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability |
| CVE-2020-0726 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-0725 | Win32k Elevation of Privilege Vulnerability                                           |
| CVE-2020-0724 | Win32k Elevation of Privilege Vulnerability                                           |

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

|               |                                                                            |
|---------------|----------------------------------------------------------------------------|
| CVE-2020-0672 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-0671 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-0670 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-0669 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-0668 | Windows Kernel Elevation of Privilege Vulnerability                        |
| CVE-2020-0667 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0666 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0665 | Active Directory Elevation of Privilege Vulnerability                      |
| CVE-2020-0664 | Active Directory Information Disclosure Vulnerability                      |
| CVE-2020-0663 | Microsoft Edge Elevation of Privilege Vulnerability                        |
| CVE-2020-0662 | Internet Connection Sharing Service Remote Code Execution Vulnerability    |
| CVE-2020-0661 | Windows Hyper-V Denial of Service Vulnerability                            |
| CVE-2020-0660 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability      |
| CVE-2020-0659 | Windows Data Sharing Service Elevation of Privilege Vulnerability          |
| CVE-2020-0658 | Windows Common Log File System Driver Information Disclosure Vulnerability |
| CVE-2020-0657 | Windows Common Log File System Driver Elevation of Privilege Vulnerability |
| CVE-2020-0655 | Remote Desktop Services Remote Code Execution Vulnerability                |
| CVE-2020-0648 | Windows RSoP Service Application Elevation of Privilege Vulnerability      |
| CVE-2020-0646 | .NET Framework Remote Code Execution Injection Vulnerability               |
| CVE-2020-0645 | Microsoft IIS Server Tampering Vulnerability                               |
| CVE-2020-0644 | Windows Elevation of Privilege Vulnerability                               |
| CVE-2020-0643 | Windows GDI+ Information Disclosure Vulnerability                          |
| CVE-2020-0642 | Win32k Elevation of Privilege Vulnerability                                |
| CVE-2020-0641 | Microsoft Windows Elevation of Privilege Vulnerability                     |
| CVE-2020-0640 | Internet Explorer Memory Corruption Vulnerability                          |
| CVE-2020-0639 | Windows Common Log File System Driver Information Disclosure Vulnerability |
| CVE-2020-0638 | Update Notification Manager Elevation of Privilege Vulnerability           |
| CVE-2020-0637 | Remote Desktop Web Access Information Disclosure Vulnerability             |
| CVE-2020-0636 | Windows Subsystem for Linux Elevation of Privilege Vulnerability           |
| CVE-2020-0635 | Windows Elevation of Privilege Vulnerability                               |
| CVE-2020-0634 | Windows Common Log File System Driver Elevation of Privilege Vulnerability |
| CVE-2020-0633 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0632 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0631 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0630 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0629 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0628 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0627 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0626 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0625 | Windows Search Indexer Elevation of Privilege Vulnerability                |
| CVE-2020-0624 | Win32k Elevation of Privilege Vulnerability                                |
| CVE-2020-0623 | Windows Search Indexer Elevation of Privilege Vulnerability                |

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

|                               |                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------|
| <a href="#">CVE-2020-0620</a> | Microsoft Cryptographic Services Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2020-0618</a> | Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability     |
| <a href="#">CVE-2020-0616</a> | Microsoft Windows Denial of Service Vulnerability                               |
| <a href="#">CVE-2020-0615</a> | Windows Common Log File System Driver Information Disclosure Vulnerability      |
| <a href="#">CVE-2020-0614</a> | Windows Search Indexer Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2020-0613</a> | Windows Search Indexer Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2020-0611</a> | Remote Desktop Client Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2020-0610</a> | Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability |
| <a href="#">CVE-2020-0609</a> | Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability |
| <a href="#">CVE-2020-0608</a> | Win32k Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2020-0607</a> | Microsoft Graphics Components Information Disclosure Vulnerability              |
| <a href="#">CVE-2020-0606</a> | .NET Framework Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2020-0605</a> | .NET Framework Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2020-0601</a> | Windows CryptoAPI Spoofing Vulnerability                                        |

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

|                               |                                                                       |
|-------------------------------|-----------------------------------------------------------------------|
| <a href="#">CVE-2019-1226</a> | Remote Desktop Services Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1225</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability   |
| <a href="#">CVE-2019-1224</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability   |
| <a href="#">.NET</a>          | Quality Rollup for .NET Framework                                     |
| <a href="#">CVE-2019-1488</a> | Microsoft Defender Security Feature Bypass Vulnerability              |
| <a href="#">CVE-2019-1485</a> | VBScript Remote Code Execution Vulnerability                          |
| <a href="#">CVE-2019-1484</a> | Windows OLE Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2019-1483</a> | Windows Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2019-1476</a> | Windows Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2019-1474</a> | Windows Kernel Information Disclosure Vulnerability                   |
| <a href="#">CVE-2019-1472</a> | Windows Kernel Information Disclosure Vulnerability                   |
| <a href="#">CVE-2019-1471</a> | Windows Hyper-V Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2019-1470</a> | Windows Hyper-V Information Disclosure Vulnerability                  |
| <a href="#">CVE-2019-1469</a> | Win32k Information Disclosure Vulnerability                           |
| <a href="#">CVE-2019-1468</a> | Win32k Graphics Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2019-1467</a> | Windows GDI Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-1466</a> | Windows GDI Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-1465</a> | Windows GDI Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-1458</a> | Win32k Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2019-1456</a> | OpenType Font Parsing Remote Code Execution Vulnerability             |
| <a href="#">CVE-2019-1453</a> | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability |
| <a href="#">CVE-2019-1439</a> | Windows GDI Information Disclosure Vulnerability                      |

|                                |                                                                          |
|--------------------------------|--------------------------------------------------------------------------|
| <a href="#">CVE-2019-1438</a>  | Windows Graphics Component Elevation of Privilege Vulnerability          |
| <a href="#">CVE-2019-1435</a>  | Windows Graphics Component Elevation of Privilege Vulnerability          |
| <a href="#">CVE-2019-1434</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1433</a>  | Windows Graphics Component Elevation of Privilege Vulnerability          |
| <a href="#">CVE-2019-1432</a>  | DirectWrite Information Disclosure Vulnerability                         |
| <a href="#">CVE-2019-1429</a>  | Scripting Engine Memory Corruption Vulnerability                         |
| <a href="#">CVE-2019-1424</a>  | NetLogon Security Feature Bypass Vulnerability                           |
| <a href="#">CVE-2019-1422</a>  | Windows Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2019-1419</a>  | OpenType Font Parsing Remote Code Execution Vulnerability                |
| <a href="#">CVE-2019-1418</a>  | Windows Modules Installer Service Information Disclosure Vulnerability   |
| <a href="#">CVE-2019-1415</a>  | Windows Installer Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2019-1412</a>  | OpenType Font Driver Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-1411</a>  | DirectWrite Information Disclosure Vulnerability                         |
| <a href="#">CVE-2019-1409</a>  | Windows Remote Procedure Call Information Disclosure Vulnerability       |
| <a href="#">CVE-2019-1408</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1407</a>  | Windows Graphics Component Elevation of Privilege Vulnerability          |
| <a href="#">CVE-2019-1406</a>  | Jet Database Engine Remote Code Execution Vulnerability                  |
| <a href="#">CVE-2019-1405</a>  | Windows UPnP Service Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2019-1399</a>  | Windows Hyper-V Denial of Service Vulnerability                          |
| <a href="#">CVE-2019-1397</a>  | Windows Hyper-V Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2019-1396</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1395</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1394</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1393</a>  | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1392</a>  | Windows Kernel Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1391</a>  | Windows Denial of Service Vulnerability                                  |
| <a href="#">CVE-2019-1390</a>  | VBScript Remote Code Execution Vulnerability                             |
| <a href="#">CVE-2019-1389</a>  | Windows Hyper-V Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2019-1388</a>  | Windows Certificate Dialog Elevation of Privilege Vulnerability          |
| <a href="#">CVE-2019-1384</a>  | Microsoft Windows Security Feature Bypass Vulnerability                  |
| <a href="#">CVE-2019-1382</a>  | Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability |
| <a href="#">CVE-2019-1381</a>  | Microsoft Windows Information Disclosure Vulnerability                   |
| <a href="#">CVE-2019-1380</a>  | Microsoft splwow64 Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2019-11135</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-0860</a>  | Chakra Scripting Engine Memory Corruption Vulnerability                  |
| <a href="#">CVE-2019-0838</a>  | Windows Information Disclosure Vulnerability                             |
| <a href="#">CVE-2019-0719</a>  | Hyper-V Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2019-0712</a>  | Windows Hyper-V Denial of Service Vulnerability                          |
| .NET                           | Quality Rollup for .NET Framework                                        |
| <a href="#">CVE-2019-1371</a>  | Internet Explorer Memory Corruption Vulnerability                        |
| <a href="#">CVE-2019-1368</a>  | Windows Secure Boot Security Feature Bypass Vulnerability                |
| <a href="#">CVE-2019-1367</a>  | Scripting Engine Memory Corruption Vulnerability                         |

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

|                               |                                                                                |
|-------------------------------|--------------------------------------------------------------------------------|
| <a href="#">CVE-2019-1366</a> | Chakra Scripting Engine Memory Corruption Vulnerability                        |
| <a href="#">CVE-2019-1365</a> | Microsoft IIS Server Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1359</a> | Jet Database Engine Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-1358</a> | Jet Database Engine Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-1357</a> | Browser Spoofing Vulnerability                                                 |
| <a href="#">CVE-2019-1356</a> | Microsoft Edge based on Edge HTML Information Disclosure Vulnerability         |
| <a href="#">CVE-2019-1347</a> | Windows Denial of Service Vulnerability                                        |
| <a href="#">CVE-2019-1346</a> | Windows Denial of Service Vulnerability                                        |
| <a href="#">CVE-2019-1345</a> | Windows Kernel Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1344</a> | Windows Code Integrity Module Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-1343</a> | Windows Denial of Service Vulnerability                                        |
| <a href="#">CVE-2019-1342</a> | Windows Error Reporting Manager Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2019-1341</a> | Windows Power Service Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2019-1340</a> | Microsoft Windows Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2019-1339</a> | Microsoft Windows Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2019-1337</a> | Windows Update Client Information Disclosure Vulnerability                     |
| <a href="#">CVE-2019-1336</a> | Microsoft Windows Update Client Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2019-1335</a> | Chakra Scripting Engine Memory Corruption Vulnerability                        |
| <a href="#">CVE-2019-1334</a> | Windows Kernel Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1333</a> | Remote Desktop Client Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2019-1326</a> | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability          |
| <a href="#">CVE-2019-1325</a> | Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability |
| <a href="#">CVE-2019-1323</a> | Microsoft Windows Update Client Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2019-1322</a> | Microsoft Windows Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2019-1321</a> | Microsoft Windows CloudStore Elevation of Privilege Vulnerability              |
| <a href="#">CVE-2019-1320</a> | Microsoft Windows Elevation of Privilege Vulnerability                         |
| <a href="#">CVE-2019-1319</a> | Windows Error Reporting Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2019-1318</a> | Microsoft Windows Transport Layer Security Spoofing Vulnerability              |
| <a href="#">CVE-2019-1317</a> | Microsoft Windows Denial of Service Vulnerability                              |
| <a href="#">CVE-2019-1315</a> | Windows Error Reporting Manager Elevation of Privilege Vulnerability           |
| <a href="#">CVE-2019-1311</a> | Windows Imaging API Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-1308</a> | Chakra Scripting Engine Memory Corruption Vulnerability                        |
| <a href="#">CVE-2019-1307</a> | Chakra Scripting Engine Memory Corruption Vulnerability                        |
| <a href="#">CVE-2019-1238</a> | VBScript Remote Code Execution Vulnerability                                   |
| <a href="#">CVE-2019-1192</a> | Microsoft Browsers Security Feature Bypass Vulnerability                       |
| <a href="#">CVE-2019-1166</a> | Windows NTLM Tampering Vulnerability                                           |
| <a href="#">CVE-2019-1060</a> | MS XML Remote Code Execution Vulnerability                                     |
| <a href="#">CVE-2019-0608</a> | Microsoft Browser Spoofing Vulnerability                                       |
| <a href="#">CVE-2019-0537</a> | Microsoft Visual Studio Information Disclosure Vulnerability                   |
| .NET                          | Preview of Quality Rollup for .NET Framework                                   |
| <a href="#">CVE-2019-1303</a> | Windows Elevation of Privilege Vulnerability                                   |
| <a href="#">CVE-2019-1300</a> | Chakra Scripting Engine Memory Corruption Vulnerability                        |

|                               |                                                                             |
|-------------------------------|-----------------------------------------------------------------------------|
| <a href="#">CVE-2019-1299</a> | Microsoft Edge based on Edge HTML Information Disclosure Vulnerability      |
| <a href="#">CVE-2019-1298</a> | Chakra Scripting Engine Memory Corruption Vulnerability                     |
| <a href="#">CVE-2019-1294</a> | Windows Secure Boot Security Feature Bypass Vulnerability                   |
| <a href="#">CVE-2019-1293</a> | Windows SMB Client Driver Information Disclosure Vulnerability              |
| <a href="#">CVE-2019-1292</a> | Windows Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2019-1291</a> | Remote Desktop Client Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2019-1290</a> | Remote Desktop Client Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2019-1289</a> | Windows Update Delivery Optimization Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2019-1287</a> | Windows Network Connectivity Assistant Elevation of Privilege Vulnerability |
| <a href="#">CVE-2019-1286</a> | Windows GDI Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1285</a> | Win32k Elevation of Privilege Vulnerability                                 |
| <a href="#">CVE-2019-1282</a> | Windows Common Log File System Driver Information Disclosure Vulnerability  |
| <a href="#">CVE-2019-1280</a> | LNK Remote Code Execution Vulnerability                                     |
| <a href="#">CVE-2019-1278</a> | Windows Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2019-1277</a> | Windows Audio Service Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2019-1274</a> | Windows Kernel Information Disclosure Vulnerability                         |
| <a href="#">CVE-2019-1273</a> | Active Directory Federation Services XSS Vulnerability                      |
| <a href="#">CVE-2019-1272</a> | Windows ALPC Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2019-1271</a> | Windows Media Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2019-1270</a> | Microsoft Windows Store Installer Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2019-1269</a> | Windows ALPC Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2019-1268</a> | Winlogon Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1267</a> | Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2019-1256</a> | Win32k Elevation of Privilege Vulnerability                                 |
| <a href="#">CVE-2019-1254</a> | Windows Hyper-V Information Disclosure Vulnerability                        |
| <a href="#">CVE-2019-1253</a> | Windows Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2019-1252</a> | Windows GDI Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1251</a> | DirectWrite Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1250</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1249</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1248</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1247</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1246</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1245</a> | DirectWrite Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1244</a> | DirectWrite Information Disclosure Vulnerability                            |
| <a href="#">CVE-2019-1243</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1242</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1241</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1240</a> | Jet Database Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1237</a> | Chakra Scripting Engine Memory Corruption Vulnerability                     |
| <a href="#">CVE-2019-1236</a> | VBScript Remote Code Execution Vulnerability                                |
| <a href="#">CVE-2019-1235</a> | Windows Text Service Framework Elevation of Privilege Vulnerability         |

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

|                               |                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------|
| <a href="#">CVE-2019-1232</a> | Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability |
| <a href="#">CVE-2019-1226</a> | Remote Desktop Services Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1225</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-1224</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-1221</a> | Scripting Engine Memory Corruption Vulnerability                                |
| <a href="#">CVE-2019-1220</a> | Microsoft Browser Security Feature Bypass Vulnerability                         |
| <a href="#">CVE-2019-1219</a> | Windows Transaction Manager Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-1217</a> | Chakra Scripting Engine Memory Corruption Vulnerability                         |
| <a href="#">CVE-2019-1216</a> | DirectX Information Disclosure Vulnerability                                    |
| <a href="#">CVE-2019-1215</a> | Windows Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2019-1214</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2019-1208</a> | VBScript Remote Code Execution Vulnerability                                    |
| <a href="#">CVE-2019-1142</a> | .NET Framework Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2019-1138</a> | Chakra Scripting Engine Memory Corruption Vulnerability                         |
| <a href="#">CVE-2019-0788</a> | Remote Desktop Client Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2019-0787</a> | Remote Desktop Client Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2018-8172</a> | Visual Studio Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2018-1037</a> | Microsoft Visual Studio Information Disclosure Vulnerability                    |
| .NET                          | Cumulative Update for Windows 10, Windows 8.1 and Windows Server 2012 R2        |
| <a href="#">CVE-2019-9518</a> | HTTP/2 Server Denial of Service Vulnerability                                   |
| <a href="#">CVE-2019-9514</a> | HTTP/2 Server Denial of Service Vulnerability                                   |
| <a href="#">CVE-2019-9513</a> | HTTP/2 Server Denial of Service Vulnerability                                   |
| <a href="#">CVE-2019-9512</a> | HTTP/2 Server Denial of Service Vulnerability                                   |
| <a href="#">CVE-2019-9511</a> | HTTP/2 Server Denial of Service Vulnerability                                   |
| <a href="#">CVE-2019-9506</a> | Encryption Key Negotiation of Bluetooth Vulnerability                           |
| <a href="#">CVE-2019-1227</a> | Windows Kernel Information Disclosure Vulnerability                             |
| <a href="#">CVE-2019-1226</a> | Remote Desktop Services Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1225</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-1224</a> | Remote Desktop Protocol Server Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-1223</a> | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability           |
| <a href="#">CVE-2019-1222</a> | Remote Desktop Services Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1212</a> | Windows DHCP Server Denial of Service Vulnerability                             |
| <a href="#">CVE-2019-1206</a> | Windows DHCP Server Denial of Service Vulnerability                             |
| <a href="#">CVE-2019-1198</a> | Microsoft Windows Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2019-1190</a> | Windows Image Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1188</a> | LNK Remote Code Execution Vulnerability                                         |
| <a href="#">CVE-2019-1187</a> | XmlLite Runtime Denial of Service Vulnerability                                 |
| <a href="#">CVE-2019-1186</a> | Windows Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2019-1184</a> | Windows Elevation of Privilege Vulnerability                                    |
| <a href="#">CVE-2019-1183</a> | Windows VBScript Engine Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1182</a> | Remote Desktop Services Remote Code Execution Vulnerability                     |
| <a href="#">CVE-2019-1181</a> | Remote Desktop Services Remote Code Execution Vulnerability                     |

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

|                               |                                                                   |
|-------------------------------|-------------------------------------------------------------------|
| <a href="#">CVE-2019-1180</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1179</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1178</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1177</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1176</a> | DirectX Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1175</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1174</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1173</a> | Windows Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-1172</a> | Windows Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-1171</a> | SymCrypt Information Disclosure Vulnerability                     |
| <a href="#">CVE-2019-1170</a> | Windows NTFS Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2019-1168</a> | Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2019-1164</a> | Windows Kernel Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2019-1163</a> | Windows File Signature Security Feature Bypass Vulnerability      |
| <a href="#">CVE-2019-1162</a> | Windows ALPC Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2019-1159</a> | Windows Kernel Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2019-1158</a> | Windows Graphics Component Information Disclosure Vulnerability   |
| <a href="#">CVE-2019-1157</a> | Jet Database Engine Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1156</a> | Jet Database Engine Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1155</a> | Jet Database Engine Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1153</a> | Microsoft Graphics Component Information Disclosure Vulnerability |
| <a href="#">CVE-2019-1152</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1151</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1150</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1149</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1148</a> | Microsoft Graphics Component Information Disclosure Vulnerability |
| <a href="#">CVE-2019-1147</a> | Jet Database Engine Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1146</a> | Jet Database Engine Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-1145</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1144</a> | Microsoft Graphics Remote Code Execution Vulnerability            |
| <a href="#">CVE-2019-1143</a> | Windows Graphics Component Information Disclosure Vulnerability   |
| <a href="#">CVE-2019-1078</a> | Microsoft Graphics Component Information Disclosure Vulnerability |
| <a href="#">CVE-2019-1057</a> | MS XML Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-0965</a> | Windows Hyper-V Remote Code Execution Vulnerability               |
| <a href="#">CVE-2019-0736</a> | Windows DHCP Client Remote Code Execution Vulnerability           |
| <a href="#">CVE-2019-0723</a> | Windows Hyper-V Denial of Service Vulnerability                   |
| <a href="#">CVE-2019-0720</a> | Hyper-V Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2019-0718</a> | Windows Hyper-V Denial of Service Vulnerability                   |
| <a href="#">CVE-2019-0717</a> | Windows Hyper-V Denial of Service Vulnerability                   |
| <a href="#">CVE-2019-0716</a> | Windows Denial of Service Vulnerability                           |
| <a href="#">CVE-2019-0715</a> | Windows Hyper-V Denial of Service Vulnerability                   |
| <a href="#">CVE-2019-0714</a> | Windows Hyper-V Denial of Service Vulnerability                   |

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

|                               |                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------|
| .NET                          | Cumulative Update for Windows 10, Windows Server 2012 R2 and Windows Server 2016 |
| <a href="#">CVE-2019-1130</a> | Windows Elevation of Privilege Vulnerability                                     |
| <a href="#">CVE-2019-1129</a> | Windows Elevation of Privilege Vulnerability                                     |
| <a href="#">CVE-2019-1128</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1127</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1126</a> | ADFS Security Feature Bypass Vulnerability                                       |
| <a href="#">CVE-2019-1124</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1123</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1122</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1121</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1120</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1119</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1118</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1117</a> | DirectWrite Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2019-1113</a> | .NET Framework Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2019-1108</a> | Remote Desktop Protocol Client Information Disclosure Vulnerability              |
| <a href="#">CVE-2019-1102</a> | GDI+ Remote Code Execution Vulnerability                                         |
| <a href="#">CVE-2019-1097</a> | DirectWrite Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2019-1096</a> | Win32k Information Disclosure Vulnerability                                      |
| <a href="#">CVE-2019-1095</a> | Windows GDI Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2019-1094</a> | Windows GDI Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2019-1093</a> | DirectWrite Information Disclosure Vulnerability                                 |
| <a href="#">CVE-2019-1091</a> | Microsoft unistore.dll Information Disclosure Vulnerability                      |
| <a href="#">CVE-2019-1090</a> | Windows RPCSS Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1089</a> | Windows RPCSS Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1088</a> | Windows Audio Service Elevation of Privilege Vulnerability                       |
| <a href="#">CVE-2019-1087</a> | Windows Audio Service Elevation of Privilege Vulnerability                       |
| <a href="#">CVE-2019-1086</a> | Windows Audio Service Elevation of Privilege Vulnerability                       |
| <a href="#">CVE-2019-1085</a> | Windows WLAN Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1083</a> | .NET Denial of Service Vulnerability                                             |
| <a href="#">CVE-2019-1082</a> | Microsoft Windows Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2019-1074</a> | Microsoft Windows Elevation of Privilege Vulnerability                           |
| <a href="#">CVE-2019-1073</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2019-1071</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2019-1067</a> | Windows Kernel Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2019-1037</a> | Windows Error Reporting Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2019-1006</a> | WCF/WIF SAML Token Authentication Bypass Vulnerability                           |
| <a href="#">CVE-2019-0975</a> | ADFS Security Feature Bypass Vulnerability                                       |
| <a href="#">CVE-2019-0966</a> | Windows Hyper-V Denial of Service Vulnerability                                  |
| <a href="#">CVE-2019-0887</a> | Remote Desktop Services Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2019-0880</a> | Microsoft splwow64 Elevation of Privilege Vulnerability                          |
| <a href="#">CVE-2019-0865</a> | SymCrypt Denial of Service Vulnerability                                         |

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

|                               |                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------|
| <a href="#">CVE-2019-0811</a> | Windows DNS Server Denial of Service Vulnerability                                |
| <a href="#">CVE-2019-0785</a> | Windows DHCP Server Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2019-0683</a> | Active Directory Elevation of Privilege Vulnerability                             |
| <a href="#">.NET</a>          | Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10, version 1809 |
| <a href="#">CVE-2019-1069</a> | Task Scheduler Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1065</a> | Windows Kernel Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1064</a> | Windows Elevation of Privilege Vulnerability                                      |
| <a href="#">CVE-2019-1053</a> | Windows Shell Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2019-1050</a> | Windows GDI Information Disclosure Vulnerability                                  |
| <a href="#">CVE-2019-1046</a> | Windows GDI Information Disclosure Vulnerability                                  |
| <a href="#">CVE-2019-1045</a> | Windows Network File System Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2019-1044</a> | Windows Secure Kernel Mode Security Feature Bypass Vulnerability                  |
| <a href="#">CVE-2019-1043</a> | Comctl32 Remote Code Execution Vulnerability                                      |
| <a href="#">CVE-2019-1041</a> | Windows Kernel Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-1040</a> | Windows NTLM Tampering Vulnerability                                              |
| <a href="#">CVE-2019-1039</a> | Windows Kernel Information Disclosure Vulnerability                               |
| <a href="#">CVE-2019-1028</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1027</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1026</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1025</a> | Windows Denial of Service Vulnerability                                           |
| <a href="#">CVE-2019-1022</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1021</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-1019</a> | Microsoft Windows Security Feature Bypass Vulnerability                           |
| <a href="#">CVE-2019-1018</a> | DirectX Elevation of Privilege Vulnerability                                      |
| <a href="#">CVE-2019-1017</a> | Win32k Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2019-1014</a> | Win32k Elevation of Privilege Vulnerability                                       |
| <a href="#">CVE-2019-1012</a> | Windows GDI Information Disclosure Vulnerability                                  |
| <a href="#">CVE-2019-1010</a> | Windows GDI Information Disclosure Vulnerability                                  |
| <a href="#">CVE-2019-1007</a> | Windows Audio Service Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-0998</a> | Windows Storage Service Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-0986</a> | Windows User Profile Service Elevation of Privilege Vulnerability                 |
| <a href="#">CVE-2019-0984</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability        |
| <a href="#">CVE-2019-0983</a> | Windows Storage Service Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-0974</a> | Jet Database Engine Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2019-0973</a> | Windows Installer Elevation of Privilege Vulnerability                            |
| <a href="#">CVE-2019-0972</a> | Local Security Authority Subsystem Service Denial of Service Vulnerability        |
| <a href="#">CVE-2019-0959</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability        |
| <a href="#">CVE-2019-0948</a> | Windows Event Viewer Information Disclosure Vulnerability                         |
| <a href="#">CVE-2019-0943</a> | Windows ALPC Elevation of Privilege Vulnerability                                 |
| <a href="#">CVE-2019-0941</a> | Microsoft IIS Server Denial of Service Vulnerability                              |
| <a href="#">CVE-2019-0909</a> | Jet Database Engine Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2019-0908</a> | Jet Database Engine Remote Code Execution Vulnerability                           |

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

|                               |                                                                            |
|-------------------------------|----------------------------------------------------------------------------|
| <a href="#">CVE-2019-0907</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0906</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0905</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0904</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0888</a> | ActiveX Data Objects (ADO) Remote Code Execution Vulnerability             |
| <a href="#">CVE-2019-0722</a> | Windows Hyper-V Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-0713</a> | Windows Hyper-V Denial of Service Vulnerability                            |
| <a href="#">CVE-2019-0711</a> | Windows Hyper-V Denial of Service Vulnerability                            |
| <a href="#">CVE-2019-0710</a> | Windows Hyper-V Denial of Service Vulnerability                            |
| <a href="#">CVE-2019-0620</a> | Windows Hyper-V Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-0981</a> | .Net Framework and .Net Core Denial of Service Vulnerability               |
| <a href="#">CVE-2019-0980</a> | .Net Framework and .Net Core Denial of Service Vulnerability               |
| <a href="#">CVE-2019-0683</a> | Active Directory Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2019-0961</a> | Windows GDI Information Disclosure Vulnerability                           |
| <a href="#">CVE-2019-0942</a> | Unified Write Filter Elevation of Privilege Vulnerability                  |
| <a href="#">CVE-2019-0936</a> | Windows Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-0931</a> | Windows Storage Service Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2019-0903</a> | GDI+ Remote Code Execution Vulnerability                                   |
| <a href="#">CVE-2019-0902</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0901</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0900</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0899</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0898</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0897</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0896</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0895</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0894</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0893</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0892</a> | Win32k Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2019-0891</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0890</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0889</a> | Jet Database Engine Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2019-0886</a> | Windows Hyper-V Information Disclosure Vulnerability                       |
| <a href="#">CVE-2019-0885</a> | Windows OLE Remote Code Execution Vulnerability                            |
| <a href="#">CVE-2019-0882</a> | Windows GDI Information Disclosure Vulnerability                           |
| <a href="#">CVE-2019-0881</a> | Windows Kernel Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2019-0864</a> | .NET Framework Denial of Service Vulnerability                             |
| <a href="#">CVE-2019-0863</a> | Windows Error Reporting Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2019-0820</a> | .NET Framework and .NET Core Denial of Service Vulnerability               |
| <a href="#">CVE-2019-0758</a> | Windows GDI Information Disclosure Vulnerability                           |
| <a href="#">CVE-2019-0734</a> | Windows Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2019-0733</a> | Windows Defender Application Control Security Feature Bypass Vulnerability |

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

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

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

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

|                               |                                                                 |
|-------------------------------|-----------------------------------------------------------------|
| <a href="#">CVE-2019-0656</a> | Windows Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2019-0637</a> | Windows Defender Firewall Security Feature Bypass Vulnerability |
| <a href="#">CVE-2019-0636</a> | Windows Information Disclosure Vulnerability                    |
| <a href="#">CVE-2019-0635</a> | Windows Hyper-V Information Disclosure Vulnerability            |
| <a href="#">CVE-2019-0633</a> | Windows SMB Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2019-0632</a> | Windows Security Feature Bypass Vulnerability                   |
| <a href="#">CVE-2019-0631</a> | Windows Security Feature Bypass Vulnerability                   |
| <a href="#">CVE-2019-0630</a> | Windows SMB Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2019-0628</a> | Win32k Information Disclosure Vulnerability                     |
| <a href="#">CVE-2019-0627</a> | Windows Security Feature Bypass Vulnerability                   |
| <a href="#">CVE-2019-0626</a> | Windows DHCP Server Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0625</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0623</a> | Win32k Elevation of Privilege Vulnerability                     |
| <a href="#">CVE-2019-0621</a> | Windows Kernel Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-0619</a> | Windows GDI Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-0618</a> | GDI+ Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2019-0616</a> | Windows GDI Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-0615</a> | Windows GDI Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-0602</a> | Windows GDI Information Disclosure Vulnerability                |
| <a href="#">CVE-2019-0601</a> | HID Information Disclosure Vulnerability                        |
| <a href="#">CVE-2019-0600</a> | HID Information Disclosure Vulnerability                        |
| <a href="#">CVE-2019-0599</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0598</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0597</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0596</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0595</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0555</a> | Microsoft XmlDocument Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2019-0584</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0583</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0582</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0581</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0580</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0579</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0578</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0577</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0576</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0575</a> | Jet Database Engine Remote Code Execution Vulnerability         |
| <a href="#">CVE-2019-0570</a> | Windows Runtime Elevation of Privilege Vulnerability            |
| <a href="#">CVE-2019-0569</a> | Windows Kernel Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-0555</a> | Microsoft XmlDocument Elevation of Privilege Vulnerability      |
| <a href="#">CVE-2019-0554</a> | Windows Kernel Information Disclosure Vulnerability             |
| <a href="#">CVE-2019-0552</a> | Windows COM Elevation of Privilege Vulnerability                |

|                               |                                                         |
|-------------------------------|---------------------------------------------------------|
| <a href="#">CVE-2019-0549</a> | Windows Kernel Information Disclosure Vulnerability     |
| <a href="#">CVE-2019-0543</a> | Microsoft Windows Elevation of Privilege Vulnerability  |
| <a href="#">CVE-2019-0538</a> | Jet Database Engine Remote Code Execution Vulnerability |
| <a href="#">CVE-2019-0536</a> | Windows Kernel Information Disclosure Vulnerability     |

## **2018 – Microsoft® Patches Tested with Pro-Watch**

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

|                               |                                                                          |
|-------------------------------|--------------------------------------------------------------------------|
| <a href="#">CVE-2018-8417</a> | Microsoft JScript Security Feature Bypass Vulnerability                  |
| <a href="#">CVE-2018-8415</a> | Microsoft PowerShell Tampering Vulnerability                             |
| <a href="#">CVE-2018-8408</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8407</a> | Remote Procedure Call runtime Information Disclosure Vulnerability       |
| <a href="#">CVE-2018-8256</a> | Microsoft PowerShell Remote Code Execution Vulnerability                 |
| <a href="#">CVE-2018-8506</a> | Microsoft Windows Codecs Library Information Disclosure Vulnerability    |
| <a href="#">CVE-2018-8497</a> | Windows Kernel Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2018-8495</a> | Windows Shell Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2018-8494</a> | MS XML Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2018-8493</a> | Windows TCP/IP Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8492</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability |
| <a href="#">CVE-2018-8489</a> | Windows Hyper-V Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2018-8486</a> | DirectX Information Disclosure Vulnerability                             |
| <a href="#">CVE-2018-8484</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8482</a> | Windows Media Player Information Disclosure Vulnerability                |
| <a href="#">CVE-2018-8481</a> | Windows Media Player Information Disclosure Vulnerability                |
| <a href="#">CVE-2018-8472</a> | Windows GDI Information Disclosure Vulnerability                         |
| <a href="#">CVE-2018-8453</a> | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2018-8423</a> | Microsoft JET Database Engine Remote Code Execution Vulnerability        |
| <a href="#">CVE-2018-8413</a> | Windows Theme API Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2018-8411</a> | NTFS Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2018-8333</a> | Microsoft Filter Manager Elevation Of Privilege Vulnerability            |
| <a href="#">CVE-2018-8330</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8329</a> | Linux On Windows Elevation Of Privilege Vulnerability                    |
| <a href="#">CVE-2018-8320</a> | Windows DNS Security Feature Bypass Vulnerability                        |
| <a href="#">CVE-2018-8475</a> | Windows Remote Code Execution Vulnerability                              |
| <a href="#">CVE-2018-8468</a> | Windows Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2018-8455</a> | Windows Kernel Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2018-8446</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8444</a> | Windows SMB Information Disclosure Vulnerability                         |
| <a href="#">CVE-2018-8443</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8442</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8440</a> | Windows ALPC Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2018-8439</a> | Windows Hyper-V Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2018-8438</a> | Windows Hyper-V Denial of Service Vulnerability                          |
| <a href="#">CVE-2018-8434</a> | Windows Hyper-V Information Disclosure Vulnerability                     |
| <a href="#">CVE-2018-8433</a> | Microsoft Graphics Component Information Disclosure Vulnerability        |
| <a href="#">CVE-2018-8424</a> | Windows GDI Information Disclosure Vulnerability                         |
| <a href="#">CVE-2018-8420</a> | MS XML Remote Code Execution Vulnerability                               |
| <a href="#">CVE-2018-8419</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8410</a> | Windows Registry Elevation of Privilege Vulnerability                    |

|                               |                                                                          |
|-------------------------------|--------------------------------------------------------------------------|
| <a href="#">CVE-2018-8393</a> | Microsoft JET Database Engine Remote Code Execution Vulnerability        |
| <a href="#">CVE-2018-8392</a> | Microsoft JET Database Engine Remote Code Execution Vulnerability        |
| <a href="#">CVE-2018-8335</a> | Windows SMB Denial of Service Vulnerability                              |
| <a href="#">CVE-2018-8332</a> | Win32k Graphics Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2018-8271</a> | Windows Information Disclosure Vulnerability                             |
| <a href="#">CVE-2018-8414</a> | Windows Shell Remote Code Execution Vulnerability                        |
| <a href="#">CVE-2018-8406</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8405</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8404</a> | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2018-8401</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8400</a> | DirectX Graphics Kernel Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8399</a> | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2018-8398</a> | Windows GDI Information Disclosure Vulnerability                         |
| <a href="#">CVE-2018-8394</a> | Windows GDI Information Disclosure Vulnerability                         |
| <a href="#">CVE-2018-8360</a> | .NET Framework Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8350</a> | Windows PDF Remote Code Execution Vulnerability                          |
| <a href="#">CVE-2018-8349</a> | Microsoft COM for Windows Remote Code Execution Vulnerability            |
| <a href="#">CVE-2018-8348</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8347</a> | Windows Kernel Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2018-8345</a> | LNK Remote Code Execution Vulnerability                                  |
| <a href="#">CVE-2018-8344</a> | Microsoft Graphics Remote Code Execution Vulnerability                   |
| <a href="#">CVE-2018-8343</a> | Windows NDIS Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2018-8341</a> | Windows Kernel Information Disclosure Vulnerability                      |
| <a href="#">CVE-2018-8340</a> | AD FS Security Feature Bypass Vulnerability                              |
| <a href="#">CVE-2018-8339</a> | Windows Installer Elevation of Privilege Vulnerability                   |
| <a href="#">CVE-2018-8204</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability |
| <a href="#">CVE-2018-8202</a> | .NET Framework Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2018-8200</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability |
| <a href="#">CVE-2018-0952</a> | Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2018-8356</a> | .NET Framework Security Feature Bypass Vulnerability                     |
| <a href="#">CVE-2018-8314</a> | Windows Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2018-8313</a> | Windows Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2018-8309</a> | Windows Denial of Service Vulnerability                                  |
| <a href="#">CVE-2018-8308</a> | Windows Kernel Elevation of Privilege Vulnerability                      |
| <a href="#">CVE-2018-8307</a> | WordPad Security Feature Bypass Vulnerability                            |
| <a href="#">CVE-2018-8304</a> | Windows DNSAPI Denial of Service Vulnerability                           |
| <a href="#">CVE-2018-8284</a> | .NET Framework Remote Code Injection Vulnerability                       |
| <a href="#">CVE-2018-8282</a> | Win32k Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2018-8260</a> | .NET Framework Remote Code Execution Vulnerability                       |
| <a href="#">CVE-2018-8242</a> | Scripting Engine Memory Corruption Vulnerability                         |
| <a href="#">CVE-2018-8222</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability |

|                               |                                                                            |
|-------------------------------|----------------------------------------------------------------------------|
| <a href="#">CVE-2018-8206</a> | Windows FTP Server Denial of Service Vulnerability                         |
| <a href="#">CVE-2018-8202</a> | .NET Framework Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2018-8251</a> | Media Foundation Memory Corruption Vulnerability                           |
| <a href="#">CVE-2018-8239</a> | Windows GDI Information Disclosure Vulnerability                           |
| <a href="#">CVE-2018-8233</a> | Win32k Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2018-8231</a> | HTTP Protocol Stack Remote Code Execution Vulnerability                    |
| <a href="#">CVE-2018-8226</a> | HTTP.sys Denial of Service Vulnerability                                   |
| <a href="#">CVE-2018-8225</a> | Windows DNSAPI Remote Code Execution Vulnerability                         |
| <a href="#">CVE-2018-8221</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2018-8219</a> | Hypervisor Code Integrity Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-8215</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2018-8214</a> | Windows Desktop Bridge Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2018-8213</a> | Windows Remote Code Execution Vulnerability                                |
| <a href="#">CVE-2018-8212</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2018-8211</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2018-8210</a> | Windows Remote Code Execution Vulnerability                                |
| <a href="#">CVE-2018-8208</a> | Windows Desktop Bridge Elevation of Privilege Vulnerability                |
| <a href="#">CVE-2018-8207</a> | Windows Kernel Information Disclosure Vulnerability                        |
| <a href="#">CVE-2018-8205</a> | Windows Denial of Service Vulnerability                                    |
| <a href="#">CVE-2018-8201</a> | Device Guard Code Integrity Policy Security Feature Bypass Vulnerability   |
| <a href="#">CVE-2018-8175</a> | WEBDAV Denial of Service Vulnerability                                     |
| <a href="#">CVE-2018-8169</a> | HIDParser Elevation of Privilege Vulnerability                             |
| <a href="#">CVE-2018-8140</a> | Cortana Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2018-8121</a> | Windows Kernel Information Disclosure Vulnerability                        |
| <a href="#">CVE-2018-0982</a> | Windows Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2018-1040</a> | Windows Code Integrity Module Denial of Service Vulnerability              |
| <a href="#">CVE-2018-1036</a> | NTFS Elevation of Privilege Vulnerability                                  |
| <a href="#">CVE-2018-1003</a> | Microsoft JET Database Engine Remote Code Execution Vulnerability          |
| <a href="#">CVE-2018-8897</a> | Windows Kernel Elevation of Privilege Vulnerability                        |
| <a href="#">CVE-2018-8174</a> | Windows VBScript Engine Remote Code Execution Vulnerability                |
| <a href="#">CVE-2018-8167</a> | Windows Common Log File System Driver Elevation of Privilege Vulnerability |
| <a href="#">CVE-2018-8166</a> | Win32k Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2018-8164</a> | Win32k Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2018-8136</a> | Windows Remote Code Execution Vulnerability                                |
| <a href="#">CVE-2018-8134</a> | Windows Elevation of Privilege Vulnerability                               |
| <a href="#">CVE-2018-8127</a> | Windows Kernel Information Disclosure Vulnerability                        |
| <a href="#">CVE-2018-8124</a> | Win32k Elevation of Privilege Vulnerability                                |
| <a href="#">CVE-2018-0959</a> | Hyper-V Remote Code Execution Vulnerability                                |
| <a href="#">CVE-2018-0824</a> | Microsoft COM for Windows Remote Code Execution Vulnerability              |
| <a href="#">CVE-2018-8116</a> | Microsoft Graphics Component Denial of Service Vulnerability               |
| <a href="#">CVE-2018-1035</a> | Windows Security Feature Bypass Vulnerability                              |

|                               |                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------|
| <a href="#">CVE-2018-1016</a> | Microsoft Graphics Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2018-1015</a> | Microsoft Graphics Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2018-1013</a> | Microsoft Graphics Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2018-1012</a> | Microsoft Graphics Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2018-1010</a> | Microsoft Graphics Remote Code Execution Vulnerability                           |
| <a href="#">CVE-2018-1009</a> | Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability |
| <a href="#">CVE-2018-1008</a> | Graphics Component Font Parsing Elevation of Privilege Vulnerability             |
| <a href="#">CVE-2018-1004</a> | Windows VBScript Engine Remote Code Execution Vulnerability                      |
| <a href="#">CVE-2018-1003</a> | Microsoft JET Database Engine Remote Code Execution Vulnerability                |
| <a href="#">CVE-2018-0976</a> | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability            |
| <a href="#">CVE-2018-0975</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0974</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0973</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0972</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0971</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0970</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0969</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0968</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0967</a> | Windows SNMP Service Denial of Service Vulnerability                             |
| <a href="#">CVE-2018-0966</a> | Device Guard Security Feature Bypass Vulnerability                               |
| <a href="#">CVE-2018-0964</a> | Hyper-V Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2018-0963</a> | Windows Kernel Elevation of Privilege Vulnerability                              |
| <a href="#">CVE-2018-0960</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0957</a> | Hyper-V Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2018-0956</a> | HTTP.sys Denial of Service Vulnerability                                         |
| <a href="#">CVE-2018-0890</a> | Active Directory Security Feature Bypass Vulnerability                           |
| <a href="#">CVE-2018-0887</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0983</a> | Windows Storage Services Elevation of Privilege Vulnerability                    |
| <a href="#">CVE-2018-0977</a> | Win32k Elevation of Privilege Vulnerability                                      |
| <a href="#">CVE-2018-0926</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0904</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0901</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0900</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0899</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0898</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0897</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0896</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0895</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0894</a> | Windows Kernel Information Disclosure Vulnerability                              |
| <a href="#">CVE-2018-0888</a> | Hyper-V Information Disclosure Vulnerability                                     |
| <a href="#">CVE-2018-0886</a> | CredSSP Remote Code Execution Vulnerability                                      |

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

|                               |                                                                |
|-------------------------------|----------------------------------------------------------------|
| <a href="#">CVE-2018-0885</a> | Windows Hyper-V Denial of Service Vulnerability                |
| <a href="#">CVE-2018-0884</a> | Windows Security Feature Bypass Vulnerability                  |
| <a href="#">CVE-2018-0883</a> | Windows Shell Remote Code Execution Vulnerability              |
| <a href="#">CVE-2018-0881</a> | Microsoft Video Control Elevation of Privilege Vulnerability   |
| <a href="#">CVE-2018-0880</a> | Windows Desktop Bridge Elevation of Privilege Vulnerability    |
| <a href="#">CVE-2018-0878</a> | Windows Remote Assistance Information Disclosure Vulnerability |
| <a href="#">CVE-2018-0868</a> | Windows Installer Elevation of Privilege Vulnerability         |
| <a href="#">CVE-2018-0817</a> | Windows GDI Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2018-0816</a> | Windows GDI Elevation of Privilege Vulnerability               |
| <a href="#">CVE-2018-0814</a> | Windows Kernel Information Disclosure Vulnerability            |
| <a href="#">CVE-2018-0813</a> | Windows Kernel Information Disclosure Vulnerability            |
| <a href="#">CVE-2018-0811</a> | Windows Kernel Information Disclosure Vulnerability            |
| <a href="#">CVE-2018-0800</a> | Scripting Engine Information Disclosure Vulnerability          |
| <a href="#">CVE-2018-0781</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0780</a> | Scripting Engine Information Disclosure Vulnerability          |
| <a href="#">CVE-2018-0778</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0777</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0776</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0800</a> | Scripting Engine Information Disclosure Vulnerability          |
| <a href="#">CVE-2018-0781</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0780</a> | Scripting Engine Information Disclosure Vulnerability          |
| <a href="#">CVE-2018-0778</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0777</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0776</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0775</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0774</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0773</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0772</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0770</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0769</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0767</a> | Scripting Engine Information Disclosure Vulnerability          |
| <a href="#">CVE-2018-0762</a> | Scripting Engine Memory Corruption Vulnerability               |
| <a href="#">CVE-2018-0758</a> | Scripting Engine Memory Corruption Vulnerability               |

---

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

|                                |                                                  |
|--------------------------------|--------------------------------------------------|
| <a href="#">CVE-2017-11918</a> | Scripting Engine Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11914</a> | Scripting Engine Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11912</a> | Scripting Engine Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11911</a> | Scripting Engine Memory Corruption Vulnerability |

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

|                                |                                                   |
|--------------------------------|---------------------------------------------------|
| <a href="#">CVE-2017-11910</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11909</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11908</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11907</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11905</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11903</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11901</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11895</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11894</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11893</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11890</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11889</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11888</a> | Microsoft Edge Memory Corruption Vulnerability    |
| <a href="#">CVE-2017-11886</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11873</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11871</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11870</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11869</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11866</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11862</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11861</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11858</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11856</a> | Internet Explorer Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11855</a> | Internet Explorer Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11846</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11845</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11843</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11841</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11840</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11839</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11838</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11837</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11836</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11822</a> | Internet Explorer Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11821</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11819</a> | Windows Shell Remote Code Execution Vulnerability |
| <a href="#">CVE-2017-11813</a> | Internet Explorer Memory Corruption Vulnerability |
| <a href="#">CVE-2017-11812</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11811</a> | Scripting Engine Memory Corruption Vulnerability  |
| <a href="#">CVE-2017-11810</a> | Scripting Engine Memory Corruption Vulnerability  |

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

|                                |                                                        |
|--------------------------------|--------------------------------------------------------|
| <a href="#">CVE-2017-11809</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11808</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11807</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11806</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11805</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11804</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11802</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11801</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11800</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11799</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11798</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11797</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11796</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11793</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11792</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11779</a> | Windows DNSAPI Remote Code Execution Vulnerability     |
| <a href="#">CVE-2017-11771</a> | Windows Search Remote Code Execution Vulnerability     |
| <a href="#">CVE-2017-11766</a> | Microsoft Edge Memory Corruption Vulnerability         |
| <a href="#">CVE-2017-11764</a> | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-11763</a> | Microsoft Graphics Remote Code Execution Vulnerability |
| <a href="#">CVE-2017-11762</a> | Microsoft Graphics Remote Code Execution Vulnerability |
| <a href="#">CVE-2017-8759</a>  | .NET Framework Remote Code Execution Vulnerability     |
| <a href="#">CVE-2017-8750</a>  | Microsoft Browser Memory Corruption Vulnerability      |
| <a href="#">CVE-2017-8749</a>  | Internet Explorer Memory Corruption Vulnerability      |
| <a href="#">CVE-2017-8748</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8747</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8741</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8740</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8737</a>  | Microsoft PDF Remote Code Execution Vulnerability      |
| <a href="#">CVE-2017-8734</a>  | Microsoft Edge Memory Corruption Vulnerability         |
| <a href="#">CVE-2017-8728</a>  | Microsoft PDF Remote Code Execution Vulnerability      |
| <a href="#">CVE-2017-8727</a>  | Windows Shell Memory Corruption Vulnerability          |
| <a href="#">CVE-2017-8727</a>  | Microsoft PDF Remote Code Execution Vulnerability      |
| <a href="#">CVE-2017-8682</a>  | Win32k Graphics Remote Code Execution Vulnerability    |
| <a href="#">CVE-2017-8674</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8672</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8671</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8670</a>  | Scripting Engine Memory Corruption Vulnerability       |
| <a href="#">CVE-2017-8669</a>  | Microsoft Browser Memory Corruption Vulnerability      |
| <a href="#">CVE-2017-8661</a>  | Microsoft Edge Memory Corruption Vulnerability         |
| <a href="#">CVE-2017-8660</a>  | Microsoft Edge Memory Corruption Vulnerability         |

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

|                               |                                                                  |
|-------------------------------|------------------------------------------------------------------|
| <a href="#">CVE-2017-8657</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8656</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8655</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8653</a> | Microsoft Browser Memory Corruption Vulnerability                |
| <a href="#">CVE-2017-8649</a> | Microsoft Browser Memory Corruption Vulnerability                |
| <a href="#">CVE-2017-8647</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8646</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8645</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8641</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8640</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8639</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8638</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8636</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8635</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8634</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8622</a> | Windows Subsystem for Linux Elevation of Privilege Vulnerability |
| <a href="#">CVE-2017-8620</a> | Windows Search Remote Code Execution Vulnerability               |
| <a href="#">CVE-2017-8619</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8618</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8617</a> | Microsoft Edge Remote Code Execution Vulnerability               |
| <a href="#">CVE-2017-8610</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8609</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8608</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8607</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8606</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8604</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8603</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8601</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8598</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8596</a> | Microsoft Edge Memory Corruption Vulnerability                   |
| <a href="#">CVE-2017-8594</a> | Internet Explorer Memory Corruption Vulnerability                |
| <a href="#">CVE-2017-8591</a> | Windows IME Remote Code Execution Vulnerability                  |
| <a href="#">CVE-2017-8589</a> | Windows Search Remote Code Execution Vulnerability               |
| <a href="#">CVE-2017-8549</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8548</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8543</a> | Windows Search Remote Code Execution Vulnerability               |
| <a href="#">CVE-2017-8528</a> | Windows Uniscribe Remote Code Execution Vulnerability            |
| <a href="#">CVE-2017-8527</a> | Windows Graphics Remote Code Execution Vulnerability             |
| <a href="#">CVE-2017-8524</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8522</a> | Scripting Engine Memory Corruption Vulnerability                 |
| <a href="#">CVE-2017-8520</a> | Scripting Engine Memory Corruption Vulnerability                 |

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

---

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

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

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

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

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

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

---

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

---

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

(974378)

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

<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)

<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)

[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

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

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

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

---

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

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

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