# 微软发布 11 月补丁修复 76 个安全问题

## 安全威胁通告

发布时间：2019 年 11 月 13 日

# 综述

微软于周二发布了 11 月安全更新补丁，修复了 76 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及 Azure Stack、Chipsets、Graphic Fonts、Microsoft Edge、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft RPC、Microsoft Scripting Engine、Microsoft Windows、Open Source Software、Servicing Stack Updates、Visual Studio、Windows Hyper-V、Windows Kernel、Windows Media Player 以及 Windows Subsystem for Linux。

相关信息如下：

| 产品 | CVE 编号 | CVE 标题 | 严重程度 |
|---|---|---|---|
| **Azure Stack** | CVE-2019-1234 | Azure Stack 欺骗漏洞 | Important |
| **Chipsets** | ADV190024 | Microsoft Guidance for Vulnerability in Trusted Platform Module (TPM) | Unknown |
| **Graphic Fonts** | CVE-2019-1456 | OpenType Font Parsing 远程代码执行漏洞 | Important |
| **Microsoft Edge** | CVE-2019-1413 | Microsoft Edge 安全功能绕过漏洞 | Important |
| **Microsoft Exchange Server** | CVE-2019-1373 | Microsoft Exchange 远程代码执行漏洞 | Critical |

| | | | |
|---|---|---|---|
| **Microsoft Graphics Component** | CVE-2019-1432 | DirectWrite 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1433 | Windows Graphics Component 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1434 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1435 | Windows Graphics Component 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1436 | Win32k 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1437 | Windows Graphics Component 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1438 | Windows Graphics Component 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1439 | Windows GDI 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Graphics Component** | CVE-2019-1440 | Win32k 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1441 | Win32k Graphics 远程代码执行漏洞 | Critical |
| **Microsoft Graphics Component** | CVE-2019-1393 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1394 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1395 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1396 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1407 | Windows Graphics Component 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Graphics Component** | CVE-2019-1408 | Win32k 特权提升漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1411 | DirectWrite 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1412 | OpenType Font Driver 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1419 | OpenType Font Parsing 远程代码执行漏洞 | Critical |
| **Microsoft JET Database Engine** | CVE-2019-1406 | Jet Database Engine 远程代码执行漏洞 | Important |
| **Microsoft Office** | CVE-2019-1457 | Microsoft Office Excel Security Feature Bypass | Important |
| **Microsoft Office** | CVE-2019-1402 | Microsoft Office 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Office** | CVE-2019-1445 | Microsoft Office Online 欺骗漏洞 | Important |
| **Microsoft Office** | CVE-2019-1446 | Microsoft Excel 信息泄露漏洞 | Important |
| **Microsoft Office** | CVE-2019-1447 | Microsoft Office Online 欺骗漏洞 | Important |
| **Microsoft Office** | CVE-2019-1448 | Microsoft Excel 远程代码执行漏洞 | Important |
| **Microsoft Office** | CVE-2019-1449 | Microsoft Office ClickToRun 安全功能绕过漏洞 | Important |
| **Microsoft Office SharePoint** | CVE-2019-1442 | Microsoft Office 安全功能绕过漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Office SharePoint** | CVE-2019-1443 | Microsoft SharePoint 信息泄露漏洞 | Important |
| **Microsoft RPC** | CVE-2019-1409 | Windows Remote Procedure Call 信息泄露漏洞 | Important |
| **Microsoft Scripting Engine** | CVE-2019-1429 | Scripting Engine 内存破坏漏洞 | Critical |
| **Microsoft Scripting Engine** | CVE-2019-1390 | VBScript 远程代码执行漏洞 | Critical |
| **Microsoft Scripting Engine** | CVE-2019-1426 | Scripting Engine 内存破坏漏洞 | Moderate |
| **Microsoft Scripting Engine** | CVE-2019-1427 | Scripting Engine 内存破坏漏洞 | Critical |
| **Microsoft Scripting Engine** | CVE-2019-1428 | Scripting Engine 内存破坏漏洞 | Critical |

| | | | |
|---|---|---|---|
| **Microsoft Windows** | CVE-2019-1374 | Windows Error Reporting 信息泄露漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1415 | Windows Installer 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1417 | Windows Data Sharing Service 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1418 | Windows Modules Installer Service 信息泄露漏洞 | Important |
| **Microsoft Windows** | CVE-2018-12207 | Windows 拒绝服务漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1324 | Windows TCP/IP 信息泄露漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1379 | Windows Data Sharing Service 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Windows** | CVE-2019-1380 | Microsoft splwow64 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1381 | Microsoft Windows 信息泄露漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1382 | Microsoft ActiveX Installer Service 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1383 | Windows Data Sharing Service 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1384 | Microsoft Windows 安全功能绕过漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1385 | Windows AppX Deployment Extensions 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Windows** | CVE-2019-1388 | Windows Certificate Dialog 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1391 | Windows 拒绝服务漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1405 | Windows UPnP Service 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1420 | Windows 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1422 | Windows 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1423 | Windows 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1424 | NetLogon 安全功能绕过漏洞 | Important |

| | | | |
|---|---|---|---|
| **Open Source Software** | CVE-2019-1370 | Open Enclave SDK 信息泄露漏洞 | Important |
| **Servicing Stack Updates** | ADV990001 | Latest Servicing Stack Updates | Critical |
| **Visual Studio** | CVE-2019-1425 | Visual Studio 特权提升漏洞 | Important |
| **Windows Hyper-V** | CVE-2019-0712 | Windows Hyper-V 拒绝服务漏洞 | Important |
| **Windows Hyper-V** | CVE-2019-0719 | Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Hyper-V** | CVE-2019-0721 | Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Hyper-V** | CVE-2019-1309 | Windows Hyper-V 拒绝服务漏洞 | Important |

| | | | |
|---|---|---|---|
| **Windows Hyper-V** | CVE-2019-1310 | Windows Hyper-V 拒绝服务漏洞 | Important |
| **Windows Hyper-V** | CVE-2019-1389 | Windows Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Hyper-V** | CVE-2019-1397 | Windows Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Hyper-V** | CVE-2019-1398 | Windows Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Hyper-V** | CVE-2019-1399 | Windows Hyper-V 拒绝服务漏洞 | Important |
| **Windows Kernel** | CVE-2019-11135 | Windows Kernel 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| **Windows Kernel** | CVE-2019-1392 | Windows Kernel 特权提升漏洞 | Important |
| **Windows Media Player** | CVE-2019-1430 | Microsoft Windows Media Foundation 远程代码执行漏洞 | Critical |
| **Windows Subsystem for Linux** | CVE-2019-1416 | Windows Subsystem for Linux 特权提升漏洞 | Important |

# 修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

# 附件

## ADV190024 - Microsoft Guidance for Vulnerability in Trusted Platform Module (TPM)

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| ADV190024<br>MITRE<br>NVD | **CVE Title:** Microsoft Guidance for Vulnerability in Trusted Platform Module (TPM)<br>**Description:**<br>Executive Summary<br>This advisory addresses CVE-2019-16863.<br>A security vulnerability exists in certain Trusted Platform Module (TPM) chipsets.Â The vulnerability weakens key confidentiality protection for a specific algorithm (ECDSA). It is important to note that this is a TPM firmware vulnerability, and not a vulnerability in the Windows operating system or a specific application. Currently no Windows | Unknown | Unknown |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | systems use the vulnerable algorithm. Other software or services you are running might use this algorithm. Therefore if your system is affected and requires the installation of TPM firmware updates, you might need to re-enroll in security services you are running to remediate those affected services. For more details contact the TPM manufacturer - https://www.st.com/tpm-update. (Please note that this article is not yet available but will be published soon. Please check back to link to the information.)<br><br>Advisory Details<br><br>**Important** This vulnerability is present in a specific vendorâ€™sÂ TPM firmware that is based on Trusted Computing Guidelines (TCG) specification family 2.0, but not 1.2, and not in the TPM standard or in Microsoft Windows. Although Windows security features do not depend on the affected algorithm, third party software may rely on keys generated by the TPM and that would be affected by the vulnerability.<br><br>Even after a TPM firmware update is installed, you might need to carry out additional remediation steps to force regeneration of previously created affected TPM keys. | | |

# FAQ

**1. What systems are at risk from these vulnerabilities?**

- **Client Operating Systems** Windows client systems are at increased risk due to the prevalence of TPM on client hardware systems. There are distinct advantages to using hardware encryption modules.
- **Server Operating Systems** Servers with TPM modules.

**2. What is a TPM?**

See Trusted Platform Module Technology Overview

**3. What is the associated CVE for this vulnerability?**

See CVE-2019-16863

**4. Have there been any active attacks detected?**

No. When this security advisory was issued, Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers.

**5. Has this vulnerability been publicly disclosed?**

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | No. Microsoft received information about the vulnerability through coordinated vulnerability disclosure.<br><br>**6. I have a Surface device. Is my device affected by this vulnerability?**<br><br>No. Microsoft Surface devices do not have these chipsets installed.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| ADV190024 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| None affected | | | | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | |

# ADV990001 - Latest Servicing Stack Updates

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| ADV990001<br>MITRE<br>NVD | **CVE Title:** Latest Servicing Stack Updates<br>**Description:**<br>This is a list of the latest servicing stack updates for each operating system. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update.<br><br>**FAQ:**<br>**1. Why are all of the Servicing Stack Updates (SSU) critical updates?**<br>The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update. | Critical | Defense in Depth |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **2. When was the most recent SSU released for each version of Microsoft Windows?**<br>Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released:<br>**Product** / **SSU Package** / **Date Released**<br>Windows Server 2008 / 4526478 / November 2019<br>Windows 7/Server 2008 R2 / 4523206 / November 2019<br>Windows Server 2012 / 4523208 / November 2019<br>Windows 8.1/Server 2012 R2 / 4524445 / November 2019<br>Windows 10 / 4523200 / November 2019<br>Windows 10 Version 1607/Server 2016 / 4520724 / November 2019<br>Windows 10 Version 1703 / 4521859 / October 2019<br>Windows 10 1709 / 4523202 / November 2019<br>Windows 10 1803/Windows Server, version 1803 / 4523203 / November 2019<br>Windows 10 1809/Server 2019 / 4523204 / November 2019<br>Windows 10 1903/Windows Server, version 1903 / 4524569 / November 2019<br>**3. Where can I find more information about the Servicing Stack Updates?** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | You can find more information by following these links:<br><br>• Servicing Stack Updates<br>• Windows 7 servicing stack updates<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>5.2 02/14/2019 08:00:00<br>In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only.<br><br>16.0 11/12/2019 08:00:00<br>A Servicing Stack Update has been released for all supported versions of Windows. See the FAQ section for more information.<br><br>15.1 10/09/2019 07:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | In the Security Updates table, corrected the KB Article Number and Download links for Server 2012, the 32-bit and x64-based versions of Windows 8.1, and Server 2012 R2. See the FAQ section for more information.<br><br>4.0 01/08/2019 08:00:00<br>A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information.<br><br>1.2 12/03/2018 08:00:00<br>FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only.<br><br>3.0 12/11/2018 08:00:00<br>A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information.<br><br>7.0 04/09/2019 07:00:00<br>A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 10 version 1809, Windows Server 2019, | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | and Windows Server 2019 (Server Core installation). See the FAQ section for more information.<br><br>3.2 12/12/2018 08:00:00<br>Fixed a typo in the FAQ.<br><br>9.0 06/11/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 10 version 1607, Windows Server 2016, Windows 10 version 1809, and Windows Server 2019. See the FAQ section for more information.<br><br>6.0 03/12/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information.<br><br>12.0 07/24/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.<br><br>10.0 06/14/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | 14.0 09/10/2019 07:00:00<br>A Servicing Stack Update has been released for all supported versions of Windows. See the FAQ section for more information.<br><br>8.0 05/14/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 10 version 1507, Windows 10 version 1607, Windows Server 2016, Windows 10 version 1703, Windows 10 version 1709, Windows Server, version 1709, Windows 10 version 1803, Windows Server, version 1803, Windows 10 version 1809, Windows Server 2019, Windows 10 version 1809 and Windows Server, version 1809. See the FAQ section for more information.<br><br>5.0 02/12/2019 08:00:00<br>A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information.<br><br>13.0 07/26/2019 07:00:00<br>A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information.<br><br>1.1 11/14/2018 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only.<br><br>2.0 12/05/2018 08:00:00<br>A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.<br><br>5.1 02/13/2019 08:00:00<br>In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only.<br><br>3.1 12/11/2018 08:00:00<br>Updated supersedence information. This is an informational change only.<br><br>1.0 11/13/2018 08:00:00<br>Information published.<br><br>11.0 07/09/2019 07:00:00<br>A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information.<br><br>15.0 10/08/2019 07:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows 7 for x64-based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2012 | 4523208 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2012 (Server Core installation) | 4523208 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows 8.1 for 32-bit systems | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 8.1 for x64-based systems | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows Server 2012 R2 | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows Server 2012 R2 (Server Core installation) | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 10 for 32-bit Systems | 4523200 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4523200 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2016 | 4521858 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4520724 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows 10 Version 1607 for x64-based Systems | 4520724 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2016 (Server Core installation) | 4521858 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4523202 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows 10 Version 1709 for x64-based Systems | 4523202 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 10 Version 1803 for 32-bit Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 10 Version 1803 for x64-based Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows Server, version 1803 (Server Core Installation) | 4521861 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows 10 Version 1809 for x64-based Systems | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows 10 Version 1809 for ARM64-based Systems | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2019 | 4521862 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2019 (Server Core installation) | 4521862 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4523202 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows 10 Version 1903 for 32-bit Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 10 Version 1903 for x64-based Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows 10 Version 1903 for ARM64-based Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Windows Server, version 1903 (Server Core installation) | 4521863 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-12207 - Windows Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2018-12207 | **CVE Title:** Windows Denial of Service Vulnerability<br>**Description:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| MITRE NVD | A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.<br><br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding.<br><br>The update addresses the vulnerability by correcting how Windows handles objects in memory.<br><br>**FAQ:**<br>**Why is Microsoft documenting a CVE that was issued by Intel?**<br><br>On November 12, 2019, Intel published a technical advisory around IntelÂ® Processor Machine Check Error vulnerability that is assigned CVE-2018-12207. Microsoft has released updates to help mitigate this vulnerability for guest Virtual Machines (VMs). By default, the protection is disabled. Enabling this protection requires action on the Host. Please follow the guidance around registry setting outlined in Microsoft Knowledge Base article 4530989 to enable this mitigation on a Hyper-V host system. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for | 4525233 Security Only | Important | Denial of Service | 4519976 | Base: 4.7<br>Temporal: 4.2 | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| Itanium-Based Systems Service Pack 1 | 4525235 Monthly Rollup | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly | Important | Denial of Service | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Denial of Service | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Denial of Service | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Denial of Service | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Denial of Service | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64- | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 4.7<br>Temporal: 4.2 | Yes |

| CVE-2018-12207 | | | | | | |
|---|---|---|---|---|---|---|
| for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0712 - Windows Hyper-V Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-0712<br>MITRE<br>NVD | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash.<br>To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash.<br>The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security | Important | Denial of Service | 4520005 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Denial of Service | 4520011 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2 | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64- | 4525234 Monthly Rollup | Important | Denial of Service | 4520002 | Base: 5.8<br>Temporal: 5.2 | Yes |

| CVE-2019-0712 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | |

# CVE-2019-0719 - Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-0719 MITRE NVD | **CVE Title:** Hyper-V Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.<br><br>The security update addresses the vulnerability by correcting how Windows Hyper-V Network Switch validates guest operating system network traffic.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 09/10/2019 07:00:00<br>Added information to the CVE article.<br><br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup | Critical | Remote Code Execution | 4520005 | Base: 8<br>Temporal: 7.2 | Yes |

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0719 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0721 - Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-0721<br>MITRE<br>NVD | **CVE Title:** Hyper-V Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.<br>An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.<br>The security update addresses the vulnerability by correcting how Windows Hyper-V Network Switch validates guest operating system network traffic.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-0721 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0721 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-0721 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-11135 - Windows Kernel Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-11135<br>MITRE<br>NVD | **CVE Title:** Windows Kernel Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.<br><br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.<br><br>The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.<br><br>**Why is Microsoft documenting a CVE that was issued by Intel?**<br><br>On November 12, 2019, Intel published a technical advisory around IntelÂ® Transactional Synchronization Extensions (IntelÂ® TSX) Transaction Asynchronous Abort vulnerability that is assigned CVE-2019-11135. Microsoft has released security updates to help mitigate this vulnerability. Please note the following:<br><br>• The operating systems protections are enabled by default for some Windows Server OS Editions. See Microsoft Knowledge Base Article 4072698 for more information.<br>• The operating systems protections are enabled by default for all Windows Client OS Editions. See Microsoft Knowledge Base Article 4073119 for more information.<br>• Customers who have elected not to enable this mitigation can alternatively choose to disable Intel's TSX feature on processors that support this action. Please see KB Microsoft Knowledge Base Article 4531006 for guidance on disabling TSX completely. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | Update | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-11135 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1234 - Azure Stack Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1234 MITRE NVD | **CVE Title:** Azure Stack Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists when Azure Stack fails to validate certain requests. An attacker who successfully exploited the vulnerability could make requests to internal Azure Stack resources. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | An attacker could exploit the vulnerability by sending a specially crafted request to the Azure Stack user portal.<br><br>The update addresses the vulnerability by changing how Azure Stack handles certain requests.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1234 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Azure Stack | Release Notes Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1309 - Windows Hyper-V Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1309<br>MITRE<br>NVD | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash.<br>To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1309 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1309 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1310 - Windows Hyper-V Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1310<br>MITRE<br>NVD | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash.<br>To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash.<br>The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1310 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector:<br>CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1310 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1310 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.8<br>Temporal: 5.2<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1324 - Windows TCP/IP Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1324 MITRE NVD | **CVE Title:** Windows TCP/IP Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles IPv6 flowlabel filled in packets. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit this vulnerability, an attacker would have to send specially crafted IPv6 packets to a remote Windows computer. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.<br><br>The update addresses the vulnerability by correcting how the Windows handles IPv6 flowlabel data in packets.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is device information like resource ids, sas tokens, user properties, and other sensitive information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1324 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.3<br>Temporal: 4.9<br>Vector: | Yes |

| CVE-2019-1324 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security | Important | Information Disclosure | 4520008 | Base: 5.3<br>Temporal: 4.9<br>Vector: | Yes |

| CVE-2019-1324 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | Update | | | | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.3<br>Temporal: 4.9<br>Vector: | Yes |

| CVE-2019-1324 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.3<br>Temporal: 4.9<br>Vector: | Yes |

| CVE-2019-1324 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.3<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |

# CVE-2019-1370 - Open Enclave SDK Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1370<br>MITRE<br>NVD | **CVE Title:** Open Enclave SDK Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information stored in the Enclave.<br>To exploit this vulnerability, an attacker would have to successfully compromise the host application running the enclave. The attacker can then pivot to the enclave and exploit this vulnerability without user interaction.<br>The security update addresses the vulnerability by modifying how Open Enclave SDK handle objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Enclave memory read - unprivileged write to enclave memory from a host application, which can leak memory contents of the enclave.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1370 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Open Enclave SDK | Release Notes Security Update | Important | Information Disclosure | | Base: 7<br>Temporal: 6.3<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:H/E:P/RL:O/RC:C | Maybe |

# CVE-2019-1373 - Microsoft Exchange Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1373<br>MITRE<br>NVD | **CVE Title:** Microsoft Exchange Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Exchange through the deserialization of metadata via PowerShell. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the logged in user.<br>Exploitation of this vulnerability requires that a user run cmdlets via PowerShell. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by correcting how Exchange serializes its metadata.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1373 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2019 Cumulative Update 2 | 4523171 Security Update | Critical | Remote Code Execution | 4515832 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 13 | 4523171 Security Update | Critical | Remote Code Execution | 4515832 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 23 | 4523171 Security Update | Critical | Remote Code Execution | 4509409 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2019 Cumulative Update 3 | 4523171 Security Update | Critical | Remote Code Execution | 4515832 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 14 | 4523171 Security Update | Critical | Remote Code Execution | 4515832 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-1374 - Windows Error Reporting Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1374<br>MITRE<br>NVD | **CVE Title:** Windows Error Reporting Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.<br>To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or convince a target to run a crafted application.<br>The security update addresses the vulnerability by correcting the way WER handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1374 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1374 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1374 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | | | | | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4523205 Security | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1374 | | | | | | |
|---|---|---|---|---|---|---|
| 1809 for ARM64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4524570 Security | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1374 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1379 - Windows Data Sharing Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1379<br>MITRE<br>NVD | **CVE Title:** Windows Data Sharing Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>An attacker could exploit this vulnerability by running a specially crafted application on the victim system.<br><br>The update addresses the vulnerability by correcting the way the Windows Data Sharing Service handles file operations.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1379 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1379 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1380 - Microsoft splwow64 Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1380<br>MITRE<br>NVD | **CVE Title:** Microsoft splwow64 Elevation of Privilege Vulnerability<br>**Description:**<br>A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited the vulnerability could elevate privileges on an affected system from low-integrity to medium-integrity.<br>This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted.<br>The security update addresses the vulnerability by ensuring splwow64.exe properly handles these calls..<br><br>**FAQ:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | 4525253 Security Only | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525246 Monthly Rollup | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64- | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64- | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1380 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1381 - Microsoft Windows Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1381 MITRE NVD | **CVE Title:** Microsoft Windows Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations. An attacker who successfully exploited the vulnerability could potentially access unauthorized files. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit this vulnerability, an authenticated attacker could run a specially crafted application in user mode.<br><br>The update addresses the vulnerability by checking files paths for symbolic links.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from the file system.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 | Important | Information Disclosure | 4520005 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| | Monthly Rollup | | | | | |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 6.6<br>Temporal: 5.9<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 6.6<br>Temporal: 5.9<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 6.6<br>Temporal: 5.9<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server | 4525243 Monthly Rollup 4525250 Security | Important | Information Disclosure | 4520005 | Base: 6.6<br>Temporal: 5.9<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | Only | | | | | |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4525241 Security | Important | Information Disclosure | 4520004 | Base: 6.6<br>Temporal: 5.9 | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| 1709 for ARM64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 6.6<br>Temporal: 5.9<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 6.6<br>Temporal: 5.9 | Yes |

| CVE-2019-1381 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 (Server Core installation) | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C | |

# CVE-2019-1382 - Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1382 MITRE NVD | **CVE Title:** Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication. An attacker who successfully exploited the vulnerability could potentially access unauthorized files.<br>To exploit this vulnerability, an authenticated attacker could run a specially crafted application on the victim system.<br>The update addresses the vulnerability by validated file permissions before accessing them. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1382 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1383 - Windows Data Sharing Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1383<br>MITRE<br>NVD | **CVE Title:** Windows Data Sharing Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br>An attacker could exploit this vulnerability by running a specially crafted application on the victim system. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses the vulnerability by correcting the way the Windows Data Sharing Service handles file operations.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1383 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1383 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1383 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1383 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1383 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1384 - Microsoft Windows Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1384<br>MITRE<br>NVD | **CVE Title:** Microsoft Windows Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.<br><br>To exploit this vulnerability, an attacker could send a specially crafted authentication request. An attacker who successfully exploited this vulnerability could access another machine using the original user privileges.<br><br>The issue has been addressed by changing how NTLM validates network authentication messages.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Security Feature Bypass | 4520007 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Security Feature Bypass | 4520007 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Security Feature Bypass | 4520005 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Security Feature Bypass | 4520005 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Security Feature Bypass | 4520005 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Security Feature Bypass | 4520005 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Security Feature Bypass | 4520005 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Security Feature Bypass | 4520011 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Security Feature Bypass | 4520011 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Security Feature Bypass | 4520002 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Security Feature Bypass | 4520002 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1384 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.5<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1385 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1385<br>MITRE<br>NVD | **CVE Title:** Windows AppX Deployment Extensions Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.<br>To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.<br>The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1385 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1385 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1385 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1385 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1385 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1388 - Windows Certificate Dialog Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1388 MITRE NVD | **CVE Title:** Windows Certificate Dialog Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br><br>The security update addresses the vulnerability by ensuring Windows Certificate Dialog properly enforces user privileges.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1388 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1389 - Windows Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1389<br>MITRE<br>NVD | **CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.<br>An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.<br>The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.<br><br>**FAQ:**<br>None | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for x64-based Systems | 4525233 Security Only 4525235 | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly | Critical | Remote Code Execution | 4520007 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server | 4525243 Monthly Rollup 4525250 | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | Security Only | | | | | |
| Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64- | 4525234 Monthly Rollup | Critical | Remote Code Execution | 4520002 | Base: 7.6<br>Temporal: 6.8 | Yes |

| CVE-2019-1389 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | |

# CVE-2019-1390 - VBScript Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1390 MITRE NVD | **CVE Title:** VBScript Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.<br><br>The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | 4525106 IE Cumulative 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on | 4525106 IE Cumulative 4525235 | Critical | Remote Code Execution | 4519976 | Base: 7.5<br>Temporal: 6.7 | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | Monthly Rollup | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525106 IE Cumulative 4525235 Monthly Rollup | Moderate | Remote Code Execution | 4519976 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows | 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Server 2012 | | | | | | |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | 4525243 Monthly Rollup 4525106 IE Cumulative | Critical | Remote Code Execution | 4519974 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525106 IE Cumulative | Critical | Remote Code Execution | 4519974 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | 4525243 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows RT 8.1 | 4525243 Monthly Rollup | Critical | Remote Code Execution | 4520005 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on | 4525236 Security Update | Moderate | Remote Code Execution | 4519998 | Base: 6.4<br>Temporal: 5.8 | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| 10 Version 1803 for 32-bit Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64- | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2019 | 4523205 Security Update | Moderate | Remote Code Execution | 4519338 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1390 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | 4525246 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1391 - Windows Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1391<br>MITRE<br>NVD | **CVE Title:** Windows Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.<br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding.<br>The update addresses the vulnerability by correcting how Windows handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Denial of Service | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Denial of Service | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Denial of Service | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Denial of Service | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Denial of Service | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based | 4525239 Security Only 4525234 | Important | Denial of Service | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Monthly Rollup | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1391 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |

# CVE-2019-1392 - Windows Kernel Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1392 MITRE NVD | **CVE Title:** Windows Kernel Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.<br>The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1392 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1392 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1392 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1392 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1393 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1393<br>MITRE<br>NVD | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1393 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1394 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1394<br>MITRE<br>NVD | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br>The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1394 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1395 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1395 | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| MITRE NVD | An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br><br>The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based | 4525239 Security Only 4525234 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Monthly Rollup | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1395 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |

# CVE-2019-1396 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1396<br>MITRE<br>NVD | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br>The update addresses this vulnerability by correcting how Win32k handles objects in memory. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1396 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1397 - Windows Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1397<br>MITRE<br>NVD | **CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.<br>An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.<br>The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.<br><br>**FAQ:**<br>None | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for x64-based Systems | 4525233 Security Only 4525235 | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly | Critical | Remote Code Execution | 4520007 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server | 4525243 Monthly Rollup 4525250 | Critical | Remote Code Execution | 4520005 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | Security Only | | | | | |
| Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1397 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.6<br>Temporal: 6.8<br>Vector:<br>CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1398 - Windows Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1398 | **CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| MITRE NVD | To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.<br><br>An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system.<br><br>The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1398 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1398 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1398 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.6<br>Temporal: 6.8<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1399 - Windows Hyper-V Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1399 MITRE NVD | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.<br><br>The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems | 4525233 Security Only 4525235 Monthly Rollup | Important | Denial of Service | 4519976 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Denial of Service | 4520007 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup | Important | Denial of Service | 4520005 | Base: 5.4<br>Temporal: 4.9 | Yes |

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Denial of Service | 4520005 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Denial of Service | 4519998 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Denial of Service | 4520004 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Denial of Service | 4520008 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.4<br>Temporal: 4.9 | Yes |

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Denial of Service | 4519338 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Denial of Service | 4517389 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1399 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Denial of Service | 4520002 | Base: 5.4<br>Temporal: 4.9<br>Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1402 - Microsoft Office Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1402 MITRE NVD | **CVE Title:** Microsoft Office Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.<br><br>The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.<br><br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1402 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484127 Security Update | Important | Information Disclosure | 4475599 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484127 Security Update | Important | Information Disclosure | 4475599 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

| CVE-2019-1402 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484119 Security Update | Important | Information Disclosure | 4475611 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484119 Security Update | Important | Information Disclosure | 4475611 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4484119 Security Update | Important | Information Disclosure | 4475611 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | 4484113 Security Update | Important | Information Disclosure | 4475591 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | 4484113 Security Update | Important | Information Disclosure | 4475591 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | 4475591 | Base: N/A Temporal: | No |

| CVE-2019-1402 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 4475591 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Information Disclosure | 4475591 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Information Disclosure | 4475591 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

# CVE-2019-1405 - Windows UPnP Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1405<br>MITRE<br>NVD | **CVE Title:** Windows UPnP Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application.<br>The update addresses the vulnerability by correcting how the Windows UPnP service accesses COM objects.<br><br>**FAQ:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems | 4525233 Security Only 4525235 | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Monthly Rollup | | | | | |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1405 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1406 - Jet Database Engine Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019- | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability<br>**Description:** | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| 1406<br>MITRE<br>NVD | A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.<br><br>An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.<br><br>The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Important | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Remote Code Execution | 4520007 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Remote Code Execution | 4520007 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Remote Code Execution | 4520005 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Remote Code Execution | 4520005 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Remote Code Execution | 4520005 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Remote Code Execution | 4520005 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Remote Code Execution | 4520005 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Remote Code Execution | 4520011 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Remote Code Execution | 4520011 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 6.7<br>Temporal: 6 | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 6.7<br>Temporal: 6 | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64- | 4525234 Monthly Rollup | Important | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6 | Yes |

| CVE-2019-1406 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 2 | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1407 - Windows Graphics Component Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1407<br>MITRE<br>NVD | **CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system.<br><br>The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1407 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1408 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1408 | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| MITRE NVD | An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br><br>The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based | 4525239 Security Only 4525234 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Monthly Rollup | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1408 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |

# CVE-2019-1409 - Windows Remote Procedure Call Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1409<br>MITRE<br>NVD | **CVE Title:** Windows Remote Procedure Call Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.<br>To exploit this vulnerability, an authenticated attacker could run a specially crafted application.<br>The update addresses the vulnerability by correcting how the Remote Procedure Call runtime initializes objects in memory. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Pack 2 (Server Core installation) | | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64- | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1409 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1411 - DirectWrite Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1411<br>MITRE<br>NVD | **CVE Title:** DirectWrite Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.<br><br>There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.<br><br>The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.4<br>Temporal: 4<br>Vector: | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security | Important | Information Disclosure | 4520008 | Base: 4.4<br>Temporal: 4<br>Vector: | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | Update | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1411 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1412 - OpenType Font Driver Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019- | **CVE Title:** OpenType Font Driver Information Disclosure Vulnerability<br>**Description:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| 1412<br>MITRE<br>NVD | An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.<br><br>To exploit this vulnerability, an attacker would have to log on to an affected system and open a document containing specially crafted fonts.<br><br>The update addresses the vulnerability by correcting how ATMFD.dll handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process.<br><br>**Mitigations:** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly | Important | Information Disclosure | 4519976 | Base: 5<br>Temporal: 4.5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 | Important | Information Disclosure | 4520007 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| | Monthly Rollup | | | | | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 5<br>Temporal: 4.5 | Yes |

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server | 4525234 Monthly | Important | Information Disclosure | 4520002 | Base: 5<br>Temporal: 4.5 | Yes |

| CVE-2019-1412 | | | | | | |
|---|---|---|---|---|---|---|
| 2008 for 32-bit Systems Service Pack 2 | Rollup 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1413 - Microsoft Edge Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1413<br>MITRE<br>NVD | **CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls. An attacker who successfully exploited this vulnerability could trick a browser into installing an extension without the user's consent.<br>To exploit the vulnerability, the user must either browse to a malicious website or be redirected to it. In an email attack scenario, an attacker could send an email message in an attempt to convince the user to click a link to a malicious site, which then can download an extension for all_urls without the user's knowledge.<br>In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of an enticement in an email or instant message. | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by correcting how Microsoft Edge handles host permissions for adding extensions.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2016 | 4525236 Security Update | Low | Security Feature Bypass | 4519998 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64- | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| for ARM64-based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2019 | 4523205 Security Update | Low | Security Feature Bypass | 4519338 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1413 | | | | | | |
|---|---|---|---|---|---|---|
| Version 1903 for 32-bit Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 4.3<br>Temporal: 3.9<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1415 - Windows Installer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1415<br>MITRE<br>NVD | **CVE Title:** Windows Installer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.<br><br>To exploit the vulnerability, an attacker would require unprivileged execution on the victim system. After successfully exploiting the vulnerability, an attacker could run arbitrary code with elevated privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>The security update addresses the vulnerability by correcting the way Windows Installer handles certain filesystem operations.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1415 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 | Security Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1416 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019- | **CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| 1416<br>MITRE<br>NVD | An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br><br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br><br>The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1416 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1416 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1416 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1416 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1417 - Windows Data Sharing Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1417<br>MITRE<br>NVD | **CVE Title:** Windows Data Sharing Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>An attacker could exploit this vulnerability by running a specially crafted application on the victim system.<br><br>The update addresses the vulnerability by correcting the way the Windows Data Sharing Service handles file operations.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | | |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64- | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1417 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1418 - Windows Modules Installer Service Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1418<br>MITRE<br>NVD | **CVE Title:** Windows Modules Installer Service Information Disclosure Vulnerability<br>**Description:**<br>An information vulnerability exists when Windows Modules Installer Service improperly discloses file information. Successful exploitation of the vulnerability could allow the attacker to read the contents of a log file on disk.<br><br>To exploit the vulnerability, an attacker would have to log onto an affected system and run a specially crafted application.<br><br>The update addresses the vulnerability by changing the way Windows Modules Installer Service discloses file information.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from the file system. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems | 4525233 Security Only | Important | Information Disclosure | 4519976 | Base: 3.5<br>Temporal: 3.2 | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4525235 Monthly Rollup | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium- | 4525233 Security Only 4525235 | Important | Information Disclosure | 4519976 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Based Systems Service Pack 1 | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Information Disclosure | 4520005 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64- | 4525232 Security | Important | Information Disclosure | 4520011 | Base: 3.5<br>Temporal: 3.2 | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | Update | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 3.5<br>Temporal: 3.2 | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 3.5<br>Temporal: 3.2 | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for | 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 3.5<br>Temporal: 3.2 | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Itanium-Based Systems Service Pack 2 | 4525234 Monthly Rollup | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based | 4525234 Monthly Rollup 4525239 | Important | Information Disclosure | 4520002 | Base: 3.5<br>Temporal: 3.2<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1418 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | Security Only | | | | | |

# CVE-2019-1419 - OpenType Font Parsing Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1419 MITRE NVD | **CVE Title:** OpenType Font Parsing Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>There are multiple ways an attacker could exploit the vulnerability, such as by either convincing a user to open a specially crafted document, or by convincing a user to visit a webpage that contains specially crafted embedded OpenType fonts.<br><br>The update addresses the vulnerability by correcting how the Windows Adobe Type Manager Library handles OpenType fonts.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Critical | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Critical | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Critical | Remote Code Execution | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Critical | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Critical | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Critical | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2019 | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Critical | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1419 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1420 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1420<br>MITRE<br>NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br><br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br><br>The security update addresses the vulnerability by ensuring the dssvc.dll properly handles this type of functionality.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-1420** | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1420 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1420 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1420 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1420 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64- | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1420 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1422 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1422 MITRE NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by ensuring the iphlpsvc.dll properly handles this type of functionality.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1422 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1423 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1423<br>MITRE<br>NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the StartTileData.dll handles file creation in protected locations. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the StartTileData.dll properly handles this type of function. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1423 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1423 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1424 - NetLogon Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1424<br>MITRE<br>NVD | **CVE Title:** NetLogon Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel. An attacker who successfully exploited the vulnerability could downgrade aspects of the connection allowing for further modification of the transmission.<br>To exploit the vulnerability, an attacker would require an active man in the middle attack to be in place for the targeted traffic.<br>The update addresses the vulnerability by modifying how Netlogon handles these connections, accounting for potential attack through a man in the middle.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Security Feature Bypass | 4519976 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly | Important | Security Feature Bypass | 4520007 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Security Feature Bypass | 4520007 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Security Feature Bypass | 4520005 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Security Feature Bypass | 4520005 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 | Important | Security Feature Bypass | 4520005 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Security Feature Bypass | 4520005 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Security Feature Bypass | 4520005 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Security Feature Bypass | 4520011 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Security Feature Bypass | 4520011 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.1<br>Temporal: 7.3 | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Security Feature Bypass | 4519998 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Security Feature Bypass | 4520008 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Security Feature Bypass | 4519338 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Security Feature Bypass | 4520004 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.1<br>Temporal: 7.3 | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Security Feature Bypass | 4517389 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Security Feature Bypass | 4520002 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1424 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Security Feature Bypass | 4520002 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1425 - Visual Studio Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1425<br>MITRE<br>NVD | **CVE Title:** Visual Studio Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when Visual Studio fails to properly validate hardlinks while extracting archived files. An attacker who successfully exploited this vulnerability could overwrite arbitrary files in the security context of the local system.<br>To exploit this vulnerability, an attacker would need to trick an elevated user into downloading a malicious package, either by getting them to open a malicious project or convincing them to add a malicious package to an existing project.<br>The vulnerabilities were introduced by NPM packages used by Visual Studio and subsequently addressed via the following two NPM advisories:<br>Arbitrary File Overwrite - tar<br>Arbitrary File Overwrite - fstream<br>The update addresses the vulnerability by updating the NPM packages, which corrects how Visual Studio validates hardlinks during extraction of file archives. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1425 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1425 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Visual Studio 2017 version 15.9 | Release Notes Security Update | Important | Elevation of Privilege | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes Security Update | Important | Elevation of Privilege | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2019 version 16.3 | Release Notes Security Update | Important | Elevation of Privilege | | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-1426 - Scripting Engine Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1426 | **CVE Title:** Scripting Engine Memory Corruption Vulnerability<br>**Description:** | Moderate | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| MITRE<br>NVD | A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.<br><br>The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 4.2<br>Temporal: 3.8<br>Vector:<br>CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2016 | 4525236 Security Update | Moderate | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| for x64-based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2019 | 4523205 Security Update | Moderate | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| Version 1709 for ARM64-based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1426 | | | | | | |
|---|---|---|---|---|---|---|
| for ARM64-based Systems | | | | | | |
| ChakraCore | Release Notes Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector:<br>CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Maybe |

# CVE-2019-1427 - Scripting Engine Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1427<br>MITRE<br>NVD | **CVE Title:** Scripting Engine Memory Corruption Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.<br><br>The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1427 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1427 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2019 | 4523205 Security Update | Moderate | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1427 | | | | | | |
|---|---|---|---|---|---|---|
| Version 1903 for x64-based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| ChakraCore | Release Notes Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Maybe |

# CVE-2019-1428 - Scripting Engine Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1428 MITRE NVD | **CVE Title:** Scripting Engine Memory Corruption Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2016 | 4525236 Security Update | Moderate | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows Server 2019 | 4523205 Security Update | Moderate | Remote Code Execution | 4519338 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| Version 1709 for ARM64-based Systems | | | | | | |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

| CVE-2019-1428 | | | | | | |
|---|---|---|---|---|---|---|
| for ARM64-based Systems | | | | | | |
| ChakraCore | Release Notes Security Update | Critical | Remote Code Execution | 4517389 | Base: 4.2<br>Temporal: 3.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Maybe |

# CVE-2019-1429 - Scripting Engine Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1429 MITRE NVD | **CVE Title:** Scripting Engine Memory Corruption Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.<br><br>The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | 4525106 IE Cumulative 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on | 4525106 IE Cumulative 4525235 | Critical | Remote Code Execution | 4519976 | Base: 7.5<br>Temporal: 6.7 | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | Monthly Rollup | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525106 IE Cumulative 4525235 Monthly Rollup | Moderate | Remote Code Execution | 4519976 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows | 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Server 2012 | | | | | | |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | 4525243 Monthly Rollup 4525106 IE Cumulative | Critical | Remote Code Execution | 4519974 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525106 IE Cumulative | Critical | Remote Code Execution | 4519974 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | 4525243 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows RT 8.1 | 4525243 Monthly Rollup | Critical | Remote Code Execution | 4520005 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | 4525232 Security Update | Critical | Remote Code Execution | 4520011 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on | 4525236 Security Update | Moderate | Remote Code Execution | 4519998 | Base: 6.4<br>Temporal: 5.8 | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Critical | Remote Code Execution | 4519998 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| 10 Version 1803 for 32-bit Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64- | 4525237 Security Update | Critical | Remote Code Execution | 4520008 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Critical | Remote Code Execution | 4519338 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2019 | 4523205 Security Update | Moderate | Remote Code Execution | 4519338 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for | 4525241 Security Update | Critical | Remote Code Execution | 4520004 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1429 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | 4525246 Monthly Rollup 4525106 IE Cumulative | Moderate | Remote Code Execution | 4519974 | Base: 6.4<br>Temporal: 5.8<br>Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1430 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1430<br>MITRE<br>NVD | **CVE Title:** Microsoft Windows Media Foundation Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files.<br><br>An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.<br><br>To exploit the vulnerability, an attacker must send a specially crafted QuickTime file to a user and convince them to open it. When opened, the malicious QuickTime file will execute code of the attackerâ€™s choice on the target system.<br><br>The security update addresses the vulnerability by ensuring Windows Media Foundation properly parses QuickTime media files. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1430 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1430 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.3<br>Temporal: 6.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.3<br>Temporal: 6.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.3<br>Temporal: 6.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Critical | Remote Code Execution | 4517389 | Base: 7.3<br>Temporal: 6.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1432 - DirectWrite Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1432<br>MITRE<br>NVD | **CVE Title:** DirectWrite Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.<br><br>There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.<br><br>The security update addresses the vulnerability by correcting how DirectWrite handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for | 4525234 Monthly | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems Service Pack 2 (Server Core installation) | Rollup 4525239 Security Only | | | | CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly | Important | Information Disclosure | 4520007 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | | |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security | Important | Information Disclosure | 4520002 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1432 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | Only | | | | | |

# CVE-2019-1433 - Windows Graphics Component Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1433 MITRE NVD | **CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64- | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1433 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |

# CVE-2019-1434 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1434<br>MITRE<br>NVD | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br>The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64- | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| based systems | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1434 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1435 - Windows Graphics Component Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019- | **CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| 1435<br>MITRE<br>NVD | An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system.<br><br>The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64- | 4525234 Monthly Rollup | Important | Elevation of Privilege | 4520002 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1435 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |

# CVE-2019-1436 - Win32k Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1436 MITRE NVD | **CVE Title:** Win32k Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.<br><br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by correcting how win32k handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4525241 Security | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| 1709 for x64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version | 4525237 Security | Important | Information Disclosure | 4520008 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 for ARM64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1436 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1437 - Windows Graphics Component Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1437<br>MITRE<br>NVD | **CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system.<br><br>The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1437 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector:<br>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1437 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1437 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1438 - Windows Graphics Component Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1438<br>MITRE<br>NVD | **CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.<br><br>In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system.<br><br>The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Important | Elevation of Privilege | 4519976 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 | Monthly Rollup | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Elevation of Privilege | 4520007 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Elevation of Privilege | 4520005 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Elevation of Privilege | 4520005 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Elevation of Privilege | 4520011 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Elevation of Privilege | 4519998 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1709 | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Elevation of Privilege | 4520008 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Elevation of Privilege | 4519338 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1709 | 4525241 Security Update | Important | Elevation of Privilege | 4520004 | Base: 7<br>Temporal: 6.3 | Yes |

| CVE-2019-1438 | | | | | | |
|---|---|---|---|---|---|---|
| for ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Elevation of Privilege | 4517389 | Base: 7<br>Temporal: 6.3<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

# CVE-2019-1439 - Windows GDI Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1439<br>MITRE<br>NVD | **CVE Title:** Windows GDI Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.<br><br>There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.<br><br>The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit | 4525233 Security | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2 | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 | Only 4525235 Monthly Rollup | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 R2 for Itanium- | 4525233 Security Only 4525235 | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Based Systems Service Pack 1 | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Information Disclosure | 4519976 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2012 | 4525253 Security Only 4525246 | Important | Information Disclosure | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| | Monthly Rollup | | | | | |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Information Disclosure | 4520007 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 8.1 for x64-based systems | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2012 R2 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2 | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Information Disclosure | 4520005 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Information Disclosure | 4520011 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2016 | 4525236 Security | Important | Information Disclosure | 4519998 | Base: 4.7<br>Temporal: 4.2 | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| | Update | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Information Disclosure | 4519998 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4525239 Security Only 4525234 Monthly | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

| CVE-2019-1439 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Rollup | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Important | Information Disclosure | 4520002 | Base: 4.7<br>Temporal: 4.2<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

# CVE-2019-1440 - Win32k Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1440<br>MITRE<br>NVD | **CVE Title:** Win32k Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.<br><br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.<br><br>The security update addresses the vulnerability by correcting how win32k handles objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1440 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version | 4525241 Security | Important | Information Disclosure | 4520004 | Base: 5<br>Temporal: 4.5 | Yes |

| CVE-2019-1440 | | | | | | |
|---|---|---|---|---|---|---|
| 1709 for 32-bit Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1440 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Information Disclosure | 4520008 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64- | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1440 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Information Disclosure | 4519338 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Information Disclosure | 4520004 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1440 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Information Disclosure | 4517389 | Base: 5<br>Temporal: 4.5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1441 - Win32k Graphics Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1441<br>MITRE<br>NVD | **CVE Title:** Win32k Graphics Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.<br>There are multiple ways an attacker could exploit this vulnerability.<br>• In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.<br>• In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file.<br><br>The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1441 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4525233 Security Only 4525235 | Critical | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1441 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Monthly Rollup | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Critical | Remote Code Execution | 4519976 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit | 4525234 Monthly Rollup | Critical | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6 | Yes |

| CVE-2019-1441 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 2 (Server Core installation) | 4525239 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4525239 Security Only 4525234 Monthly Rollup | Critical | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems | 4525234 Monthly Rollup 4525239 Security | Critical | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1441 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4525234 Monthly Rollup 4525239 Security Only | Critical | Remote Code Execution | 4520002 | Base: 6.7<br>Temporal: 6<br>Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1442 - Microsoft Office Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1442 MITRE NVD | **CVE Title:** Microsoft Office Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists when Microsoft Office does not validate URLs. | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials. An attacker who successfully exploited this vulnerability could perform a phishing attack.<br><br>The update addresses the vulnerability by ensuring Microsoft Office properly validates URLs.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector.<br><br>**There are multiple update packages available for some of the affected software. Do I need to install all the updates listed in the Security Updates table for the software?**<br><br>Yes. Customers should apply all updates offered for the software installed on their systems. If multiple updates apply, they can be installed in any order.<br><br>**Mitigations:**<br>None<br>**Workarounds:** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1442 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Server 2019 | 4484142 Security Update<br>4484149 Security Update | Important | Security Feature Bypass | 4464557 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2019-1443 - Microsoft SharePoint Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1443<br>MITRE<br>NVD | **CVE Title:** Microsoft SharePoint Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Microsoft SharePoint when an attacker uploads a specially crafted file to the SharePoint Server.<br>An authenticated attacker who successfully exploited this vulnerability could potentially leverage SharePoint functionality to obtain SMB hashes.<br>The security update addresses the vulnerability by correcting how SharePoint checks file content.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from the file system. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1443 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1443 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft SharePoint Foundation 2010 Service Pack 2 | 4484165 Security Update | Important | Information Disclosure | 4484131 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Foundation 2013 Service Pack 1 | 4484157 Security Update | Important | Information Disclosure | 4484122 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | 4484143 Security Update | Important | Information Disclosure | 4484111 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Server 2019 | 4484142 Security Update | Important | Information Disclosure | 4484110 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-1445 - Microsoft Office Online Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1445<br>MITRE<br>NVD | **CVE Title:** Microsoft Office Online Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications handlers correctly. An attacker could exploit the vulnerability by sending a specially crafted request to an affected site.<br>The attacker who successfully exploited the vulnerability could then perform cross-origin attacks on affected systems. These attacks could allow the attacker to read content that the attacker is not authorized to read, and use the victim's identity to take actions on the site on behalf of the victim. The victim needs to be authenticated for an attacker to compromise the victim.<br>The security update addresses the vulnerability by ensuring that Office Online properly validates origins.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-1445** | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Office Online Server | 4484141 Security Update | Important | Spoofing | 4475595 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2019-1446 - Microsoft Excel Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1446<br>MITRE<br>NVD | **CVE Title:** Microsoft Excel Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data.<br><br>To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created.<br><br>The update addresses the vulnerability by changing the way certain Excel functions handle objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | 4484164 Security Update | Important | Information Disclosure | 4484130 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | 4484164 Security Update | Important | Information Disclosure | 4484130 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484160 Security Update | Important | Information Disclosure | 4475569 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484160 Security Update | Important | Information Disclosure | 4475569 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484152 Security Update | Important | Information Disclosure | 4475558 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484152 Security Update | Important | Information Disclosure | 4475558 | Base: N/A Temporal: | Maybe |

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2013 RT Service Pack 1 | 4484152 Security Update | Important | Information Disclosure | 4475558 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | 4484158 Security Update | Important | Information Disclosure | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | 4484158 Security Update | Important | Information Disclosure | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4484158 Security Update | Important | Information Disclosure | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2016 for Mac | Release Notes Security Update | Important | Information Disclosure | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Excel 2016 (32-bit edition) | 4484144 Security Update | Important | Information Disclosure | 4484112 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | 4484144 Security Update | Important | Information Disclosure | 4484112 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | 4484148 Security Update | Important | Information Disclosure | 4475554 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | 4484148 Security Update | Important | Information Disclosure | 4475554 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | 4484151 Security Update | Important | Information Disclosure | 4462215 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | 4462215 | Base: N/A Temporal: | No |

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 4462215 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Information Disclosure | 4462215 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Information Disclosure | 4462215 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Information Disclosure | 4462215 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |
| Microsoft Office Online Server | 4484141 Security Update | Important | Information Disclosure | 4475595 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

| CVE-2019-1446 | | | | | | |
|---|---|---|---|---|---|---|
| Excel Services on Microsoft SharePoint Server 2010 Service Pack 2 | 4484159 Security Update | Important | Information Disclosure | 4462176 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2019-1447 - Microsoft Office Online Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1447<br>MITRE<br>NVD | **CVE Title:** Microsoft Office Online Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications handlers correctly. An attacker could exploit the vulnerability by sending a specially crafted request to an affected site.<br>The attacker who successfully exploited the vulnerability could then perform cross-origin attacks on affected systems. These attacks could allow the attacker to read content that the attacker is not authorized to read, and use the victim's identity to take actions on the site on behalf of the victim. The victim needs to be authenticated for an attacker to compromise the victim. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The security update addresses the vulnerability by ensuring that Office Online properly validates origins.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1447 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Office Online Server | 4484141 Security Update | Important | Spoofing | 4475595 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2019-1448 - Microsoft Excel Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1448<br>MITRE<br>NVD | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.<br><br>Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.<br><br>The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-1448** | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | 4484164 Security Update | Important | Remote Code Execution | 4484130 | Base: N/A<br>Temporal: | Maybe |

| CVE-2019-1448 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | 4484164 Security Update | Important | Remote Code Execution | 4484130 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | 4484158 Security Update | Important | Remote Code Execution | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | 4484158 Security Update | Important | Remote Code Execution | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4484158 Security Update | Important | Remote Code Execution | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Remote Code Execution | 4484123 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

| CVE-2019-1448 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Excel 2016 (32-bit edition) | 4484144 Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | 4484144 Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4484112 | Base: N/A Temporal: | No |

| CVE-2019-1448 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4484112 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | No |

# CVE-2019-1449 - Microsoft Office ClickToRun Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1449<br>MITRE<br>NVD | **CVE Title:** Microsoft Office ClickToRun Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists in the way that Office Click-to-Run (C2R) components handle a specially crafted file, which could lead to a standard user, any AppContainer sandbox, and Office LPAC Protected View to escalate privileges to SYSTEM. | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | To exploit this bug, an attacker would have to run a specially crafted file. The security update addresses how C2R components handle these files.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1449 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-1456 - OpenType Font Parsing Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1456 MITRE NVD | **CVE Title:** OpenType Font Parsing Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>There are multiple ways an attacker could exploit the vulnerability, such as by either convincing a user to open a specially crafted document, or by convincing a user to visit a webpage that contains specially crafted embedded OpenType fonts.<br>The update addresses the vulnerability by correcting how the Windows Adobe Type Manager Library handles OpenType fonts. | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4525233 Security Only 4525235 Monthly Rollup | Important | Remote Code Execution | 4519976 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2012 | 4525253 Security Only 4525246 Monthly Rollup | Important | Remote Code Execution | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4525253 Security Only 4525246 Monthly Rollup | Important | Remote Code Execution | 4520007 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4525250 Security Only 4525243 Monthly Rollup | Important | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64- | 4525243 Monthly Rollup | Important | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| based systems | 4525250 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 R2 | 4525243 Monthly Rollup 4525250 Security Only | Important | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4525243 Monthly Rollup | Important | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4525243 Monthly Rollup 4525250 Security Only | Important | Remote Code Execution | 4520005 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4525232 Security Update | Important | Remote Code Execution | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4525232 Security Update | Important | Remote Code Execution | 4520011 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4525236 Security Update | Important | Remote Code Execution | 4519998 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| 1803 (Server Core Installation) | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4525237 Security Update | Important | Remote Code Execution | 4520008 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2019 | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4523205 Security Update | Important | Remote Code Execution | 4519338 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | 4525241 Security Update | Important | Remote Code Execution | 4520004 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524570 Security Update | Important | Remote Code Execution | 4517389 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4525239 Security Only 4525234 Monthly | Important | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Rollup | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4525234 Monthly Rollup 4525239 Security Only | Important | Remote Code Execution | 4520002 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1456 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |

# CVE-2019-1457 - Microsoft Office Excel Security Feature Bypass

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1457<br>MITRE<br>NVD | **CVE Title:** Microsoft Office Excel Security Feature Bypass<br>**Description:**<br>A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run. Â  To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Microsoft Office software. Â  The security update addresses the vulnerability by enforcing macro settings on Excel documents.<br><br>**FAQ:** | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Is the Preview Pane an attack vector for this vulnerability?**<br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 11/12/2019 08:00:00<br>Information published. | | |

# Affected Software

The following tables list the affected software details for the vulnerability.

| CVE-2019-1457 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1457 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Security Feature Bypass | | Base: N/A Temporal: N/A Vector: N/A | No |

## 声 明

==========

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

## 关于绿盟科技

==========

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码