# 微软发布 12 月补丁修复 38 个安全问题

## 安全威胁通告


发布时间：2019 年 12 月 11 日

# 综述

微软于周二发布了 12 月安全更新补丁，修复了 38 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 End of Life Software、Microsoft Graphics Component、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows、None、Open Source Software、Servicing Stack Updates、Skype for Business、SQL Server、Visual Studio、Windows Hyper-V、Windows Kernel、Windows Media Player 以及 Windows OLE。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞共有 7 个，分别存在于 Hyper-V、Windows font library 以及 Visual Studio 中。除此之外，还包含多个重要（Important）漏洞。

# Critical 漏洞概述

以下为此次更新中包含的 7 个 Critical 级别漏洞。

## CVE-2019-1468

这是 Windows 字体库（font library）中的一个远程执行代码漏洞，源于该库无法正确处理某些嵌入式字体。 攻击者可以通过在网页上使用特制的恶意嵌入字体来利用此漏洞，诱使用户访问该网页或者在其计算机上打开特制字体文件，从而远程执行代码。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468

## CVE-2019-1471

这是 Hyper-V 虚拟机管理程序中的远程代码执行漏洞。 Hyper-V 有时可能无法正确验证 guest 操作系统上经过身份验证的用户的输入。 攻击者可以通过在 guest OS 上运行经过特殊设计的应用程序来利用此漏洞，这将使 Hyper-V host OS 在 host 操作系统上执行任意代码。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1471

## Visual Studio

Git for Visual Studio 中存在多个关键漏洞（CVE-2019-1349、CVE-2019-1350、CVE-2019-1352、CVE-2019-1354、CVE-2019-1387）。

Git for Visual Studio 过滤输入时存在问题，可能导致一个远程执行代码漏洞。 成功利用此漏洞的攻击者可以控制受影响的系统。 然后，攻击者可能会安装程序，查看，更改或删除数据； 或创建具有完全用户权限的新帐户。
要利用此漏洞，攻击者首先需要说服用户克隆恶意存储库。
关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1349

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1350
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1352
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1354
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1387

# Important 漏洞概述

除了 2 个 Critical 漏洞外，此次更新还包含了多个 important 级别漏洞，其中 3 个较需关注的漏洞如下。

## CVE-2019-1458

这是 Windows Win32k 组件中的特权提升漏洞。 攻击者可以通过登录系统，然后运行经过特殊设计的应用程序来利用此漏洞，从而使他们可以完全控制系统并以内核模式执行任意代码。 Microsoft 报告说此漏洞已被广泛在野利用。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1458

## CVE-2019-1469

这是 Windows 中的一个信息泄露漏洞，源于 win32k 组件有时无法提供内核信息。 攻击者可以利用此漏洞获取未初始化的内存和内核内存，然后将其用于其他攻击。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1469

## CVE-2019-1485

这是 VBscript 引擎中的一个远程执行代码漏洞。 攻击者可以利用此漏洞来破坏受影响系统的内存，使他们可以在当前用户的上下文中执行任意代码。 要触发此漏洞，用户必须在 Internet Explorer Web 浏览器中访问恶意的，经过特殊设计的网站。 攻击者还可能在使用 Internet Explorer 呈现引擎的应用程序或 Microsoft Office 文档中嵌入标记为"初始化安全"的 ActiveX 控件，然后诱使用户打开该文件。

关于漏洞的更多详情及更新下载，请参考微软官方安全通告：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1485

# 修复概况

本次更新的漏洞修复情况见下表：

| 产品 | CVE 编号 | CVE 标题 | 严重程度 |
| --- | --- | --- | --- |
| **End of Life Software** | CVE-2019-1489 | Remote Desktop Protocol 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1465 | Windows GDI 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1466 | Windows GDI 信息泄露漏洞 | Important |
| **Microsoft Graphics Component** | CVE-2019-1467 | Windows GDI 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Graphics Component** | CVE-2019-1468 | Win32k Graphics 远程代码执行漏洞 | Critical |
| **Microsoft Office** | CVE-2019-1400 | Microsoft Access 信息泄露漏洞 | Important |
| **Microsoft Office** | CVE-2019-1461 | Microsoft Word 拒绝服务漏洞 | Important |
| **Microsoft Office** | CVE-2019-1462 | Microsoft PowerPoint 远程代码执行漏洞 | Important |
| **Microsoft Office** | CVE-2019-1463 | Microsoft Access 信息泄露漏洞 | Important |
| **Microsoft Office** | CVE-2019-1464 | Microsoft Excel 信息泄露漏洞 | Important |
| **Microsoft Scripting Engine** | CVE-2019-1485 | VBScript 远程代码执行漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Windows** | CVE-2019-1453 | Windows Remote Desktop Protocol (RDP) 拒绝服务漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1474 | Windows Kernel 信息泄露漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1483 | Windows 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1488 | Microsoft Defender 安全功能绕过漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1476 | Windows 特权提升漏洞 | Important |
| **Microsoft Windows** | CVE-2019-1477 | Windows Printer Service 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| **Microsoft Windows** | CVE-2019-1478 | Windows COM Server 特权提升漏洞 | Important |
| **None** | ADV190026 | Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business | |
| **Open Source Software** | CVE-2019-1487 | Microsoft Authentication Library for Android 信息泄露漏洞 | Important |
| **Servicing Stack Updates** | ADV990001 | Latest Servicing Stack Updates | Critical |
| **Skype for Business** | CVE-2019-1490 | Skype for Business Server 欺骗漏洞 | Important |
| **SQL Server** | CVE-2019-1332 | Microsoft SQL Server Reporting Services XSS Vulnerability | Important |

| | | | |
|---|---|---|---|
| **Visual Studio** | CVE-2019-1349 | Git for Visual Studio 远程代码执行漏洞 | Critical |
| **Visual Studio** | CVE-2019-1350 | Git for Visual Studio 远程代码执行漏洞 | Critical |
| **Visual Studio** | CVE-2019-1351 | Git for Visual Studio Tampering Vulnerability | Moderate |
| **Visual Studio** | CVE-2019-1352 | Git for Visual Studio 远程代码执行漏洞 | Critical |
| **Visual Studio** | CVE-2019-1354 | Git for Visual Studio 远程代码执行漏洞 | Critical |
| **Visual Studio** | CVE-2019-1387 | Git for Visual Studio 远程代码执行漏洞 | Critical |

| | | | |
|---|---|---|---|
| **Visual Studio** | CVE-2019-1486 | Visual Studio Live Share 欺骗漏洞 | Important |
| **Windows Hyper-V** | CVE-2019-1470 | Windows Hyper-V 信息泄露漏洞 | Important |
| **Windows Hyper-V** | CVE-2019-1471 | Windows Hyper-V 远程代码执行漏洞 | Critical |
| **Windows Kernel** | CVE-2019-1472 | Windows Kernel 信息泄露漏洞 | Important |
| **Windows Kernel** | CVE-2019-1458 | Win32k 特权提升漏洞 | Important |
| **Windows Kernel** | CVE-2019-1469 | Win32k 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| **Windows Media Player** | CVE-2019-1480 | Windows Media Player 信息泄露漏洞 | Important |
| **Windows Media Player** | CVE-2019-1481 | Windows Media Player 信息泄露漏洞 | Important |
| **Windows OLE** | CVE-2019-1484 | Windows OLE 远程代码执行漏洞 | 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

## ADV190026 - Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| ADV190026<br>MITRE<br>NVD | **CVE Title:** Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business<br>**Description:**<br>Microsoft is aware of an issue in Windows Hello for Business (WHfB) with public keys that persist after a device is removed from Active Directory, if the AD exists. After a user sets up Windows Hello for Business (WHfB), the WHfB public key is written to the on-premises Active Directory. The WHfB keys are tied to a user and a device that has been added to Azure AD, and if the device is removed, the corresponding WHfB key is considered orphaned. However, these orphaned keys are not deleted even | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | when the device it was created on is no longer present. Any authentication to Azure AD using such an orphaned WHfB key will be rejected. However, some of these orphaned keys could lead to the following security issue in Active Directory 2016 or 2019, in either hybrid or on-premises environments.<br><br>An authenticated attacker could obtain orphaned keys created on TPMs that were affected by CVE-2017-15361 (ROCA), discussed in Microsoft Security Advisory ADV170012 to compute their WHfB private key from the orphaned public keys. The attacker could then impersonate the user by using the stolen private key to authenticate as the user within the domain using Public Key Cryptography for Initial Authentication (PKINIT).<br><br>This attack is possible even if firmware and software updates have been applied to TPMs that were affected by CVE-2017-15361 because the corresponding public keys might still exist in Active Directory.<br><br>This advisory provides guidance for cleaning up any orphaned public keys that were generated with an unpatched TPM (before firmware updates discussed in ADV170012 were applied). Follow this guidance to identify and remove orphaned WHfB keys.<br><br>This particular issue with orphaned public keys can be present when WHfB is set up in the following configurations: | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | • WHfB is deployed on Active Directory 2016 or 2019, either in hybrid mode or on-premises only.<br>• Currently have or have had in the past, WHfB keys generated on TPMs that were affected by CVE-2017-15361.<br><br>**Important**: Azure Active Directory (Azure AD) and Active Directory Federation Services (AD FS) are not affected by this issue. However, we strongly recommend that you follow the **Recommended Actions** section of ADV170012, and apply any firmware updates supplied by your TPM OEM, to avoid any exposure to Azure AD and AD FS. See Step #4 of the **Recommended Actions** for a list of OEMs and links to information for their updates.<br><br>**FAQ:**<br>**1. What systems are at risk?**<br>Individual machines or servers are not affected by this WHfB issue. Affected environments are defined in the **Mitigations** section of this advisory.<br>**2. Has this issue been publicly disclosed?**<br>Yes, this issue has been disclosed. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | **3. Have there been any active attacks detected?**<br><br>No. When this security advisory was issued, Microsoft had not received any information to indicate that this issue had been publicly used to attack customers.<br><br>**4. How do I know if my TPMs are affected by CVE-2017-15361? How do I fix them?**<br><br>Please refer to Microsoft Security Advisory ADV170012 for more details on CVE-2017-15361. You must follow the guidance in ADV170012 and update your TPMs before applying the mitigations for identifying and removing the orphaned public keys.<br><br>**5. I have updated all of my TPMs that were affected by CVE-2017-15361 with firmware provided by the OEM. Are my systems still affected?**<br><br>Yes. Orphaned WHFB keys previously generated from those TPMs could still be stored in Active Directory.<br><br>**6. My TPMs are not affected by CVE-2017-15361, but I do not enforce a policy to use TPMs for WHfB. Am I still affected?**<br><br>In the absence of a hardware-required policy, WHFB will prefer using the TPM for storing the private key. If you do not have any TPMs that are affected by CVE-2017-15361, then you are not impacted. However, we recommend removing any orphaned | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | keys in your directory by following the steps discussed in the **Mitigations** section of this advisory.<br><br>**7. I am running pre-2016 versions of Active Directory. Do I also need to remove these orphaned keys?**<br><br>While you are not affected by this WHFB issue, we strongly recommend removing these orphaned keys as a security hygiene measure.<br><br>**8. I regularly audit and clean up stale devices in my environment. How did I end up with orphaned keys?**<br><br>When a user provisions a WHFB credential, the public key is stored in the msDS-KeyCredentialLink attribute of the user object in Azure AD and on-premises Active Directory. If the device that was used to create the key is removed from Azure AD and Active Directory, the WHFB public key created for the user on that device is not automatically removed from the user object and it becomes an orphaned key.<br><br>**9. I have deployed WHFB certificate trust in my environment and use certificates for authentication. Am I affected? Do I need to remove orphaned keys?** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Yes. You are still affected by this issue if you have deployed certificate trust and have 2016 or 2019 DCs in your environment. These DC versions still support key-based authentication even if you have deployed end user certificates for authentication.<br><br>**Mitigations:**<br><br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/03/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| ADV190026 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| ADV190026 | | | | | | |
|---|---|---|---|---|---|---|
| None Available | | | | | 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 |

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td></td><td>
2. When was the most recent SSU released for each version of Microsoft Windows?<br><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><br>
<table>
<tr><th>Product</th><th>SSU Package</th><th>Date Released</th></tr>
<tr><td>Windows Server 2008</td><td>4531787</td><td>December 2019</td></tr>
<tr><td>Windows 7/Server 2008 R2</td><td>4531786</td><td>December 2019</td></tr>
<tr><td>Windows Server 2012</td><td>4532920</td><td>December 2019</td></tr>
<tr><td>Windows 8.1/Server 2012 R2</td><td>4524445</td><td>November 2019</td></tr>
<tr><td>Windows 10</td><td>4523200</td><td>November 2019</td></tr>
<tr><td>Windows 10 Version 1607/Server 2016</td><td>4520724</td><td>November 2019</td></tr>
<tr><td>Windows 10 Version 1703</td><td>4521859</td><td>October 2019</td></tr>
<tr><td>Windows 10 1709</td><td>4523202</td><td>November 2019</td></tr>
<tr><td>Windows 10 1803/Windows Server, version 1803</td><td>4523203</td><td>November 2019</td></tr>
<tr><td>Windows 10 1809/Server 2019</td><td>4523204</td><td>November 2019</td></tr>
<tr><td>Windows 10 1903/Windows Server, version 1903</td><td>4524569</td><td>November 2019</td></tr>
</table>
3. Where can I find more information about the Servicing Stack Updates?
</td><td></td><td></td></tr>
</table>

| 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>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>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>6.0 03/12/2019 07:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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>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>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>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.<br><br>13.0 07/26/2019 07:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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>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>15.0 10/08/2019 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>15.1 10/09/2019 07:00:00<br>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>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>1.0 11/13/2018 08:00:00<br>Information published. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 1.1 11/14/2018 08:00:00<br>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>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>3.1 12/11/2018 08:00:00<br>Updated supersedence information. This is an informational change only.<br><br>3.2 12/12/2018 08:00:00<br>Fixed a typo in the FAQ.<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>5.0 02/12/2019 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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>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>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, and Windows Server 2019 (Server Core installation). See the FAQ section for more information.<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>12.0 07/24/2019 07:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | 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>16.1 11/13/2019 08:00:00<br>Fixed some incorrect KB numbers. This is an information change only.<br><br>17.0 12/10/2019 08:00:00<br>A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 7, Windows Server 2008 R2, and Windows Server 2008 R2 (Server Core installation). 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** |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1803 for x64-based Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4523203 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| 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 | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | Yes |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows 10 Version 1809 for ARM64-based Systems | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2019 | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2019 (Server Core installation) | 4523204 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4523202 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| 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 | Yes |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4523202 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for 32-bit Systems | 4523200 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for x64-based Systems | 4523200 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 | Yes |
| 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 | Yes |
| Windows Server 2016 | 4520724 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | Yes |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows Server 2016 (Server Core installation) | 4520724 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows 7 for 32-bit Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| 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 | Yes |
| 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 | Yes |

| 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 | Yes |
| 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 | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4526478 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| 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 | Yes |
| 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 | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: | Yes |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4523206 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| 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<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2012 | 4523208 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2012 (Server Core installation) | 4523208 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Windows Server 2012 R2 | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| ADV990001 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4524445 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server, version 1903 (Server Core installation) | 4524569 Servicing Stack Update | Critical | Defense in Depth | | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2019-1332 - Microsoft SQL Server Reporting Services XSS Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1332<br>MITRE<br>NVD | **CVE Title:** Microsoft SQL Server Reporting Services XSS Vulnerability<br>**Description:**<br>A cross-site scripting (XSS) vulnerability exists when Microsoft SQL Server Reporting Services (SSRS) does not properly sanitize a specially-crafted web request to an affected SSRS server. An attacker who successfully exploited the vulnerability could run scripts in the context of the targeted user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.<br>To exploit the vulnerability, an attacker would need to convince an authenticated user to click a specially-crafted link to an affected SSRS server.<br>The update addresses the vulnerability by correcting SSRS URL sanitization.<br><br>**FAQ:** | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1332 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| SQL Server 2017 Reporting Services | Release Notes Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1332 | | | | | | |
|---|---|---|---|---|---|---|
| Power BI Report Server | Release Notes Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| SQL Server 2019 Reporting Services | Release Notes Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1349 - Git for Visual Studio Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1349<br>MITRE<br>NVD | **CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. An attacker who successfully exploited this 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. Users whose accounts are | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | 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 would first need to convince the user to clone a malicious repo.<br><br>The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br><br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1349 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1349 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1350 - Git for Visual Studio Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1350<br>MITRE<br>NVD | **CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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>To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo.<br><br>The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br><br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1350 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: | Yes |

| CVE-2019-1350 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1351 - Git for Visual Studio Tampering Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1351<br>MITRE<br>NVD | **CVE Title:** Git for Visual Studio Tampering Vulnerability<br>**Description:**<br>A tampering vulnerability exists when Git for Visual Studio improperly handles virtual drive paths. An attacker who successfully exploited this vulnerability could write arbitrary | Moderate | Tampering |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | files and directories to certain locations on a vulnerable system. However, an attacker would have limited control over the destination of the files and directories.<br><br>To exploit the vulnerability, an attacker must clone a file using a specially crafted path on a vulnerable system.<br><br>The security update fixes the vulnerability by ensuring Git for Visual Studio properly handles folder paths.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br><br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1351 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Moderate | Tampering | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Moderate | Tampering | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1351 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Visual Studio 2017 version 16.0 | Release Notes<br>Security Update | Moderate | Tampering | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Moderate | Tampering | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1352 - Git for Visual Studio Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1352<br>MITRE<br>NVD | **CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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>To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo.<br><br>The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br><br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1352 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: | Yes |

| CVE-2019-1352 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1354 - Git for Visual Studio Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1354 | **CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability<br>**Description:** | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| MITRE NVD | A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. An attacker who successfully exploited this 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. 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 would first need to convince the user to clone a malicious repo.<br><br>The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br><br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1354 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: | Yes |

| CVE-2019-1354 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1387 - Git for Visual Studio Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1387<br>MITRE<br>NVD | **CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. An attacker who successfully exploited this 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. 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>To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo.<br>The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input.<br><br>**FAQ:** | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1387 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2017 version 15.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1400 - Microsoft Access Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1400<br>MITRE<br>NVD | **CVE Title:** Microsoft Access Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Microsoft Access 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.<br><br>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 Access 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.<br><br>**Mitigations:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1400 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1400 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2016 (32-bit edition) | 4484180 Security Update | Important | Information Disclosure | 4484113 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2016 (64-bit edition) | 4484180 Security Update | Important | Information Disclosure | 4484113 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484193 Security Update | Important | Information Disclosure | 4484127 | Base: N/A Temporal: | Yes |

| CVE-2019-1400 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484193 Security Update | Important | Information Disclosure | 4484127 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2013 RT Service Pack 1 | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1453 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1453<br>MITRE<br>NVD | **CVE Title:** Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RDP service on the target system to stop responding.<br>To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services.<br>The update addresses the vulnerability by correcting how RDP handles connection requests.<br><br>**FAQ:**<br>None<br>**Mitigations:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1909 (Server Core installation) | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for x64-based Systems | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530717 Security Update | Important | Denial of Service | 4525237 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4530717 Security Update | Important | Denial of Service | 4525237 | Base: 7.5<br>Temporal: 6.7 | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows Server, version 1803 (Server Core Installation) | 4530717 Security Update | Important | Denial of Service | 4525237 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530717 Security Update | Important | Denial of Service | 4525237 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530715 Security Update | Important | Denial of Service | 4523205 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | 4530715 Security Update | Important | Denial of Service | 4523205 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4530715 Security Update | Important | Denial of Service | 4523205 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4530715 Security Update | Important | Denial of Service | 4523205 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Important | Denial of Service | 4523205 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530714 Security Update | Important | Denial of Service | 4525241 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530714 Security Update | Important | Denial of Service | 4525241 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4530714 Security Update | Important | Denial of Service | 4525241 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Denial of Service | 4524570 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4530681 Security Update | Important | Denial of Service | 4525232 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4530681 Security Update | Important | Denial of Service | 4525232 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530689 Security Update | Important | Denial of Service | 4525236 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530689 Security Update | Important | Denial of Service | 4525236 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4530689 Security Update | Important | Denial of Service | 4525236 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4530689 Security Update | Important | Denial of Service | 4525236 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Denial of Service | 4525235 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Denial of Service | 4525235 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4530702 Monthly Rollup | Important | Denial of Service | 4525243 | Base: 7.5<br>Temporal: 6.7 | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| | 4530730 Security Only | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows 8.1 for x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Denial of Service | 4525243 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4530702 Monthly Rollup | Important | Denial of Service | 4525243 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Denial of Service | 4525235 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Denial of Service | 4525235 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/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) | 4530734 Monthly Rollup 4530692 Security Only | Important | Denial of Service | 4525235 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Denial of Service | 4525246 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1453 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Important | Denial of Service | 4525246 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security Only | Important | Denial of Service | 4525243 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4530702 Monthly Rollup 4530730 Security Only | Important | Denial of Service | 4525243 | Base: 7.5<br>Temporal: 6.7<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1458 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1458<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | 4530681 Security Update | Important | Elevation of Privilege | 4525232 | Base: 7.8<br>Temporal: 7.2<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows 10 for x64- | 4530681 Security Update | Important | Elevation of Privilege | 4525232 | Base: 7.8<br>Temporal: 7.2 | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | |
| Windows 10 Version 1607 for 32-bit Systems | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2016 | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows 7 for 32-bit Systems | 4530734 Monthly Rollup 4530692 | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Security Only | | | | | |
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Elevation of Privilege | 4525243 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Elevation of Privilege | 4525243 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4530702 Monthly Rollup | Important | Elevation of Privilege | 4525243 | Base: 7.8<br>Temporal: 7.2 | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security | Important | Elevation of Privilege | 4525246 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |

| CVE-2019-1458 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Important | Elevation of Privilege | 4525246 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security Only | Important | Elevation of Privilege | 4525243 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | 4530702 Monthly Rollup 4530730 Security Only | Important | Elevation of Privilege | 4525243 | Base: 7.8<br>Temporal: 7.2<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Yes |

# CVE-2019-1461 - Microsoft Word Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1461<br>MITRE<br>NVD | **CVE Title:** Microsoft Word Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists in Microsoft Word software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could cause a remote denial of service against a system.<br>Exploitation of the vulnerability requires that a specially crafted document be sent to a vulnerable user.<br>The security update addresses the vulnerability by correcting how Microsoft Word handles objects in memory.<br>**FAQ:**<br>**I have Microsoft Word 2010 installed. Why am I not being offered the 4475598 update?**<br>The 4475598 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1461 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: | Yes |

| CVE-2019-1461 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Word 2016 (32-bit edition) | 4484169 Security Update | Important | Denial of Service | 4475540 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Word 2016 (64-bit edition) | 4484169 Security Update | Important | Denial of Service | 4475540 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1461 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4475598 Security Update | Important | Denial of Service | 4475531 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4475598 Security Update | Important | Denial of Service | 4475531 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Word 2010 Service Pack 2 (32-bit editions) | 4475601 Security Update | Important | Denial of Service | 4475533 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Word 2010 Service Pack 2 (64-bit editions) | 4475601 Security Update | Important | Denial of Service | 4475533 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Word 2013 RT Service Pack 1 | 4484094 Security Update | Important | Denial of Service | 4475547 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Word 2013 Service Pack 1 (32-bit editions) | 4484094 Security Update | Important | Denial of Service | 4475547 | Base: N/A Temporal: | Yes |

| CVE-2019-1461 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Word 2013 Service Pack 1 (64-bit editions) | 4484094 Security Update | Important | Denial of Service | 4475547 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1462 - Microsoft PowerPoint Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1462<br>MITRE<br>NVD | **CVE Title:** Microsoft PowerPoint Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft PowerPoint 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 control of the affected system. An attacker could then install programs; view, change, or | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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 Office PowerPoint software. 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) that contains 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>Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Microsoft PowerPoint handles objects in memory.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?** | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1462 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: | Yes |

| CVE-2019-1462 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions) | 4461590 Security Update | Important | Remote Code Execution | 4461481 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1462 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions) | 4461590 Security Update | Important | Remote Code Execution | 4461481 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft PowerPoint 2013 RT Service Pack 1 | 4461590 Security Update | Important | Remote Code Execution | 4461481 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft PowerPoint 2016 (32-bit edition) | 4484166 Security Update | Important | Remote Code Execution | 4461532 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft PowerPoint 2016 (64-bit edition) | 4484166 Security Update | Important | Remote Code Execution | 4461532 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Remote Code Execution | 4461532 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions) | 4461613 Security Update | Important | Remote Code Execution | 4461521 | Base: N/A Temporal: | Yes |

| CVE-2019-1462 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions) | 4461613 Security Update | Important | Remote Code Execution | 4461521 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1463 - Microsoft Access Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1463<br>MITRE<br>NVD | **CVE Title:** Microsoft Access Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Microsoft Access 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.<br>To exploit the 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 Microsoft Access handles objects in memory.<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1463 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2016 (32-bit edition) | 4484180 Security Update | Important | Information Disclosure | 4484113 | Base: N/A Temporal: N/A Vector: N/A | Yes |

| CVE-2019-1463 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2016 (64-bit edition) | 4484180 Security Update | Important | Information Disclosure | 4484113 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484193 Security Update | Important | Information Disclosure | 4484127 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484193 Security Update | Important | Information Disclosure | 4484127 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2013 RT Service Pack 1 | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484186 Security Update | Important | Information Disclosure | 4484119 | Base: N/A Temporal: | Yes |

| CVE-2019-1463 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |

# CVE-2019-1464 - Microsoft Excel Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1464<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>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>The update addresses the vulnerability by changing the way certain Excel functions handle objects in memory.<br><br>**FAQ:** | 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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1464 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1464 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Information Disclosure | | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Excel 2016 (32-bit edition) | 4484179 Security Update | Important | Information Disclosure | 4484144 | Base: N/A Temporal: | Yes |

| CVE-2019-1464 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Excel 2016 (64-bit edition) | 4484179 Security Update | Important | Information Disclosure | 4484144 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2016 (32-bit edition) | 4484182 Security Update | Important | Information Disclosure | 4484148 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2016 (64-bit edition) | 4484182 Security Update | Important | Information Disclosure | 4484148 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Information Disclosure | 4484148 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | 4484196 Security Update | Important | Information Disclosure | 4484164 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

| CVE-2019-1464 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | 4484196 Security Update | Important | Information Disclosure | 4484164 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Excel 2013 RT Service Pack 1 | 4484190 Security Update | Important | Information Disclosure | 4484158 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | 4484190 Security Update | Important | Information Disclosure | 4484158 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | 4484190 Security Update | Important | Information Disclosure | 4484158 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484192 Security Update | Important | Information Disclosure | 4484160 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484192 Security Update | Important | Information Disclosure | 4484160 | Base: N/A Temporal: | Yes |

| CVE-2019-1464 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2013 RT Service Pack 1 | 4484184 Security Update | Important | Information Disclosure | 4484152 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484184 Security Update | Important | Information Disclosure | 4484152 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484184 Security Update | Important | Information Disclosure | 4484152 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1465 - Windows GDI Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1465<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1909 for | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1803 for x64-based Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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) | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530715 Security | Important | Information Disclosure | 4523205 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| 1809 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 1809 for x64-based Systems | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1709 for 32-bit Systems | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| (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 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 x64- | 4530702 Monthly | Important | Information Disclosure | 4525243 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| based systems | Rollup 4530730 Security Only | | | | 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 RT 8.1 | 4530702 Monthly Rollup | Important | Information Disclosure | 4525243 | 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 Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security | Important | Information Disclosure | 4525234 | 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-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Only | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup | Important | Information Disclosure | 4525235 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems Service Pack 1 (Server Core installation) | 4530692 Security Only | | | | 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 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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 | 4530702 Monthly Rollup 4530730 | Important | Information Disclosure | 4525243 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1465 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | 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 2012 R2 (Server Core installation) | 4530702 Monthly Rollup<br>4530730 Security Only | Important | Information Disclosure | 4525243 | 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-2019-1466 - Windows GDI Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1466<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. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Installation ) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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- | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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) | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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) | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 | 4530702 Monthly Rollup | Important | Information Disclosure | 4525243 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Itanium- | 4530734 Monthly Rollup 4530692 | Important | Information Disclosure | 4525235 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Based Systems Service Pack 1 | Security Only | | | | 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 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 Core installation) | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 | 4530702 Monthly Rollup 4530730 Security | Important | Information Disclosure | 4525243 | 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-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | Only | | | | | |
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for ARM64- | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1466 | | | | | | |
|---|---|---|---|---|---|---|
| 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 | |

# CVE-2019-1467 - Windows GDI Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1467 MITRE 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>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>The security update addresses the vulnerability by correcting how the Windows GDI component handles 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 uninitialized memory.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server, version 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for ARM64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1803 for 32-bit Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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) | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-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 1809 for 32-bit Systems | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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) | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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- | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1903 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows 10 for 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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) | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 | 4530702 Monthly Rollup | Important | Information Disclosure | 4525243 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup | Important | Information Disclosure | 4525234 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems Service Pack 2 | 4530719 Security Only | | | | 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 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 Core installation) | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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-2019-1467 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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) | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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-2019-1468 - Win32k Graphics Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1468<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1909 for x64-based Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1909 (Server Core installation) | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.4<br>Temporal: 7.6 | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530714 Security Update | Critical | Remote Code Execution | 4525241 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/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 | 4530714 Security Update | Critical | Remote Code Execution | 4525241 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530714 Security Update | Critical | Remote Code Execution | 4525241 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/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 | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530681 Security Update | Critical | Remote Code Execution | 4525232 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64- | 4530681 Security Update | Critical | Remote Code Execution | 4525232 | Base: 8.4<br>Temporal: 7.6 | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/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 | 4530689 Security Update | Critical | Remote Code Execution | 4525236 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530689 Security Update | Critical | Remote Code Execution | 4525236 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | 4530689 Security Update | Critical | Remote Code Execution | 4525236 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530689 Security Update | Critical | Remote Code Execution | 4525236 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for 32-bit Systems | 4530734 Monthly Rollup 4530692 | Critical | Remote Code Execution | 4525235 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Security Only | | | | | |
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Critical | Remote Code Execution | 4525235 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530702 Monthly Rollup 4530730 Security Only | Critical | Remote Code Execution | 4525243 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530702 Monthly Rollup 4530730 Security Only | Critical | Remote Code Execution | 4525243 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4530702 Monthly Rollup | Critical | Remote Code Execution | 4525243 | Base: 8.4<br>Temporal: 7.6 | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Critical | Remote Code Execution | 4525234 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530695 Monthly Rollup 4530719 Security Only | Critical | Remote Code Execution | 4525234 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530695 Monthly Rollup 4530719 Security Only | Critical | Remote Code Execution | 4525234 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Critical | Remote Code Execution | 4525234 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530695 Monthly Rollup 4530719 Security Only | Critical | Remote Code Execution | 4525234 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530734 Monthly Rollup 4530692 Security Only | Critical | Remote Code Execution | 4525235 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Critical | Remote Code Execution | 4525235 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530734 Monthly Rollup 4530692 Security Only | Critical | Remote Code Execution | 4525235 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security | Critical | Remote Code Execution | 4525246 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1468 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Critical | Remote Code Execution | 4525246 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security Only | Critical | Remote Code Execution | 4525243 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530702 Monthly Rollup 4530730 Security Only | Critical | Remote Code Execution | 4525243 | Base: 8.4<br>Temporal: 7.6<br>Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1469 - Win32k Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1469<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for | 4530717 Security Update | Important | Information Disclosure | 4525237 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1803 for x64-based Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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) | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530715 Security | Important | Information Disclosure | 4523205 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| 1809 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 1809 for x64-based Systems | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1709 for 32-bit Systems | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| (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 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 x64- | 4530702 Monthly | Important | Information Disclosure | 4525243 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| based systems | Rollup 4530730 Security Only | | | | 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 RT 8.1 | 4530702 Monthly Rollup | Important | Information Disclosure | 4525243 | 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 Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security | Important | Information Disclosure | 4525234 | 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-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Only | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup | Important | Information Disclosure | 4525235 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems Service Pack 1 (Server Core installation) | 4530692 Security Only | | | | 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 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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 | 4530702 Monthly Rollup 4530730 | Important | Information Disclosure | 4525243 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | 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 2012 R2 (Server Core installation) | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 1909 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 (Server | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1469 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1470 - Windows Hyper-V Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1470 MITRE NVD | **CVE Title:** Windows Hyper-V Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information.<br><br>An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V 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>**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 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 12/10/2019 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-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for x64-based Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 | 4530717 Security Update | Important | Information Disclosure | 4525237 | Base: 6<br>Temporal: 5.4<br>Vector: | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core Installation) | | | | | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for x64-based Systems | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Important | Information Disclosure | 4523205 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for | 4530714 Security | Important | Information Disclosure | 4525241 | Base: 6<br>Temporal: 5.4<br>Vector: | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | Update | | | | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 6<br>Temporal: 5.4<br>Vector: | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows Server 2016 | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security | Important | Information Disclosure | 4525234 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | Only | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/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) | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security | Important | Information Disclosure | 4525243 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1470 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 (Server Core installation) | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 6<br>Temporal: 5.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-1471 - Windows Hyper-V Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1471<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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1471 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.2<br>Temporal: 7.4<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1471 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows Server, version 1803 (Server Core Installation) | 4530717 Security Update | Critical | Remote Code Execution | 4525237 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/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 | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530715 Security Update | Critical | Remote Code Execution | 4523205 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1471 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/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) | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1909 (Server Core installation) | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for x64-based Systems | 4530684 Security Update | Critical | Remote Code Execution | 4524570 | Base: 8.2<br>Temporal: 7.4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1472 - Windows Kernel Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1472<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>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for ARM64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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) | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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- | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1472 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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) | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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-2019-1474 - Windows Kernel Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1474 MITRE 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>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 | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - 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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Installation ) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4530717 Security Update | Important | Information Disclosure | 4525237 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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- | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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) | 4530715 Security Update | Important | Information Disclosure | 4523205 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4530714 Security Update | Important | Information Disclosure | 4525241 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 32-bit Systems | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530681 Security Update | Important | Information Disclosure | 4525232 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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) | 4530689 Security Update | Important | Information Disclosure | 4525236 | 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 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 | 4530702 Monthly Rollup | Important | Information Disclosure | 4525243 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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) | 4530695 Monthly Rollup 4530719 Security Only | Important | Information Disclosure | 4525234 | 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 Itanium- | 4530734 Monthly Rollup 4530692 | Important | Information Disclosure | 4525235 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Based Systems Service Pack 1 | Security Only | | | | 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 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 Core installation) | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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) | 4530691 Monthly Rollup 4530698 Security Only | Important | Information Disclosure | 4525246 | 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 | 4530702 Monthly Rollup 4530730 Security Only | Important | Information Disclosure | 4525243 | 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 | 4530702 Monthly Rollup 4530730 Security | Important | Information Disclosure | 4525243 | 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-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | Only | | | | | |
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 (Server Core installation) | 4530684 Security Update | Important | Information Disclosure | 4524570 | 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 1909 for ARM64- | 4530684 Security Update | Important | Information Disclosure | 4524570 | Base: 5.5<br>Temporal: 5<br>Vector: | Yes |

| CVE-2019-1474 | | | | | | |
|---|---|---|---|---|---|---|
| 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 | |

# CVE-2019-1476 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1476 MITRE NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. 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.<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 security update addresses the vulnerability by correcting how Windows AppX Deployment Service handles hard links. | 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 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 for 32-bit Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 for x64-based Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 (Server Core installation) | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4530714 Security Update | Important | Elevation of Privilege | 4525241 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530714 Security Update | Important | Elevation of Privilege | 4525241 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| 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 Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1476 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4530689 Security Update | Important | Elevation of Privilege | 4525236 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1477 - Windows Printer Service Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1477 MITRE NVD | **CVE Title:** Windows Printer Service Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers. An authenticated attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. | 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 update addresses this vulnerability by correcting how the Windows Printer Service validates file paths.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1477 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1477 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1478 - Windows COM Server Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1478<br>MITRE<br>NVD | **CVE Title:** Windows COM Server Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when Windows improperly handles COM object creation. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges.<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 the vulnerability by correcting how the Windows COM Server creates COM objects.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1478 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1478 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530695 Monthly Rollup 4530719 Security | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1478 | | | | | | |
|---|---|---|---|---|---|---|
| 2 (Server Core installation) | Only | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Elevation of Privilege | 4525234 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1478 | | | | | | |
|---|---|---|---|---|---|---|
| 2 (Server Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530734 Monthly Rollup 4530692 Security | Important | Elevation of Privilege | 4525235 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1478 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 (Server Core installation) | Only | | | | | |

# CVE-2019-1480 - Windows Media Player Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1480 MITRE NVD | **CVE Title:** Windows Media Player Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Windows Media Player 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.<br>To exploit this vulnerability, an attacker would have to log on to an affected system and open a specifically crafted file. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | The update addresses the vulnerability by correcting how Windows Media Player 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.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1480 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1481 - Windows Media Player Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1481<br>MITRE<br>NVD | **CVE Title:** Windows Media Player Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in Windows Media Player 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.<br>To exploit this vulnerability, an attacker would have to log on to an affected system and open a specifically crafted file.<br>The update addresses the vulnerability by correcting how Windows Media Player 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 uninitialized memory.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1481 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |

| CVE-2019-1481 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Information Disclosure | 4525235 | 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-2019-1483 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1483 | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| MITRE<br>NVD | To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges.<br><br>The security update addresses the vulnerability by correcting how AppX Deployment Server handles junctions.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1483 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 (Server Core installation) | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 for x64-based Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 1909 for 32-bit Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1483 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530717 Security Update | Important | Elevation of Privilege | 4525237 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1483 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4530715 Security Update | Important | Elevation of Privilege | 4523205 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1483 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4530714 Security Update | Important | Elevation of Privilege | 4525241 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530714 Security Update | Important | Elevation of Privilege | 4525241 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530714 Security Update | Important | Elevation of Privilege | 4525241 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2019-1483 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | | |
| Windows 10 Version 1903 for ARM64-based Systems | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4530684 Security Update | Important | Elevation of Privilege | 4524570 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-1484 - Windows OLE Remote Code Execution Vulnerability

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

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| 1484<br>MITRE<br>NVD | A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code.<br><br>To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file or a program, causing Windows to execute arbitrary code.<br><br>The update addresses the vulnerability by correcting how Windows OLE validates user input.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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 | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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 1803 (Server | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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 | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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 | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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 ARM64- | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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) | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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 | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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 | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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 | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 x64-based Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 | 4530681 Security Update | Important | Remote Code Execution | 4525232 | 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 x64-based Systems | 4530681 Security Update | Important | Remote Code Execution | 4525232 | 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 | 4530689 Security Update | Important | Remote Code Execution | 4525236 | 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 | 4530689 Security Update | Important | Remote Code Execution | 4525236 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| x64-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 2016 | 4530689 Security Update | Important | Remote Code Execution | 4525236 | 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) | 4530689 Security Update | Important | Remote Code Execution | 4525236 | 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 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Remote Code Execution | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security Only | Important | Remote Code Execution | 4525235 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Remote Code Execution | 4525243 | 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-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Remote Code Execution | 4525243 | 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 | 4530702 Monthly Rollup | Important | Remote Code Execution | 4525243 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Remote Code Execution | 4525234 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Remote Code Execution | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Remote Code Execution | 4525234 | 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 | 4530695 Monthly Rollup 4530719 Security Only | Important | Remote Code Execution | 4525234 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4530695 Monthly Rollup 4530719 Security Only | Important | Remote Code Execution | 4525234 | 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 Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Remote Code Execution | 4525235 | 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 | 4530734 Monthly Rollup 4530692 Security | Important | Remote Code Execution | 4525235 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | Only | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4530734 Monthly Rollup 4530692 Security Only | Important | Remote Code Execution | 4525235 | 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 | 4530691 Monthly Rollup 4530698 Security Only | Important | Remote Code Execution | 4525246 | 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) | 4530691 Monthly Rollup 4530698 Security | Important | Remote Code Execution | 4525246 | 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-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security Only | Important | Remote Code Execution | 4525243 | 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) | 4530702 Monthly Rollup 4530730 Security Only | Important | Remote Code Execution | 4525243 | 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 1909 (Server Core installation) | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 1909 for | 4530684 Security Update | Important | Remote Code Execution | 4524570 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2019-1484 | | | | | | |
|---|---|---|---|---|---|---|
| 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 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 1909 for x64-based Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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-2019-1485 - VBScript Remote Code Execution Vulnerability

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

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| 1485<br>MITRE<br>NVD | 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 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 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| **CVE-2019-1485** | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 10 on Windows | 4530691 Monthly Rollup 4530677 IE | Low | Remote Code Execution | 4525106 | Base: 6.4<br>Temporal: 5.8<br>Vector:<br>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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Server 2012 | Cumulative | | | | | |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530677 IE Cumulative 4530695 Monthly Rollup | Low | Remote Code Execution | 4525234 | 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 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4530677 IE Cumulative 4530695 Monthly Rollup | Low | Remote Code Execution | 4525234 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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 x64-based Systems | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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 | 4530717 Security Update | Important | Remote Code Execution | 4525237 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| 10 Version 1803 for ARM64-based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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- | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | 4530715 Security Update | Important | Remote Code Execution | 4523205 | 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 | 4530715 Security Update | Low | Remote Code Execution | 4523205 | 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 | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Version 1709 for 32-bit Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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 ARM64- | 4530714 Security Update | Important | Remote Code Execution | 4525241 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 | 4530681 Security Update | Important | Remote Code Execution | 4525232 | 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- | 4530681 Security Update | Important | Remote Code Execution | 4525232 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | 4530689 Security Update | Important | Remote Code Execution | 4525236 | 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 | 4530689 Security Update | Important | Remote Code Execution | 4525236 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows Server 2016 | 4530689 Security Update | Low | Remote Code Execution | 4525236 | 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 | 4530677 IE Cumulative 4530734 Monthly Rollup | Important | Remote Code Execution | 4525235 | 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 7 for x64-based Systems | 4530677 IE Cumulative 4530734 Monthly Rollup | Important | Remote Code Execution | 4525235 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | 4530677 IE Cumulative 4530702 Monthly Rollup | Important | Remote Code Execution | 4525243 | 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 | 4530677 IE Cumulative 4530702 Monthly Rollup | Important | Remote Code Execution | 4525243 | 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 RT 8.1 | 4530702 Monthly Rollup | Important | Remote Code Execution | 4525243 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530677 IE Cumulative 4530734 Monthly Rollup | Low | Remote Code Execution | 4525235 | 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 Server 2012 | 4530677 IE Cumulative | Low | Remote Code Execution | 4525106 | 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 Server 2012 R2 | 4530677 IE Cumulative 4530702 Monthly Rollup | Low | Remote Code Execution | 4525243 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 1909 for ARM64-based Systems | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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 | 4530684 Security Update | Important | Remote Code Execution | 4524570 | 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-2019-1485 | | | | | | |
|---|---|---|---|---|---|---|
| 10 Version 1909 for x64-based Systems | | | | | | |

# CVE-2019-1486 - Visual Studio Live Share Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1486 MITRE NVD | **CVE Title:** Visual Studio Live Share Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists in Visual Studio Live Share when a guest connected to a Live Share session is redirected to an arbitrary URL specified by the session host. An attacker who successfully exploited this vulnerability could cause a connected guest's computer to open a browser and navigate to a URL without consent from the guest.<br>To exploit the vulnerability, an attacker would need to host a Live Share session and convince a targeted user to connect to the session. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | The update addresses the vulnerability by prompting the Live Share guest for consent prior to browsing to the host-specified URL.<br><br>**FAQ:**<br>**I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?**<br>No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1486 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) | Release Notes<br>Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio Live Share extension | Release Notes<br>Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |
| Microsoft Visual Studio 2019 version 16.0 | Release Notes<br>Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

# CVE-2019-1487 - Microsoft Authentication Library for Android Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1487<br>MITRE<br>NVD | **CVE Title:** Microsoft Authentication Library for Android Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability in Android Apps using Microsoft Authentication Library (MSAL) 0.3.1-Alpha or later exists under specific conditions. This vulnerability could result in sensitive data being exposed.<br>To exploit this vulnerability an attacker would need to be authenticated to have rights to view the sensitive data.<br>This security update addresses the vulnerability by modifying how the data is sanitized.<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 sensitive information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1487 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Authentication Library (MSAL) for Android | Github Repository Security Update | Important | Information Disclosure | | Base: N/A Temporal: | Yes |

| CVE-2019-1487 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |

# CVE-2019-1488 - Microsoft Defender Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1488<br>MITRE<br>NVD | **CVE Title:** Microsoft Defender Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists when Microsoft Defender improperly handles specific buffers. An attacker could exploit the vulnerability to trigger warnings and false positives when no threat is present.<br>To exploit the vulnerability, an attacker would first require execution permissions on the victim system.<br>The security update addresses the vulnerability by ensuring Microsoft Defender properly handles these buffers.<br><br>**FAQ:** | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4530717 Security Update | Important | Security Feature Bypass | 4525237 | Base: 3.3<br>Temporal: 3<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4530717 Security Update | Important | Security Feature Bypass | 4525237 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | 4530717 Security Update | Important | Security Feature Bypass | 4525237 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | 4530717 Security Update | Important | Security Feature Bypass | 4525237 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | 4530715 Security Update | Important | Security Feature Bypass | 4523205 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64- | 4530715 Security Update | Important | Security Feature Bypass | 4523205 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1809 for ARM64-based Systems | 4530715 Security Update | Important | Security Feature Bypass | 4523205 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | 4530715 Security Update | Important | Security Feature Bypass | 4523205 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | 4530715 Security Update | Important | Security Feature Bypass | 4523205 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | 4530714 Security Update | Important | Security Feature Bypass | 4525241 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64- | 4530714 Security Update | Important | Security Feature Bypass | 4525241 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1709 for ARM64-based Systems | 4530714 Security Update | Important | Security Feature Bypass | 4525241 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for 32-bit Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for x64-based Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4530681 Security Update | Important | Security Feature Bypass | 4525232 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | 4530681 Security Update | Important | Security Feature Bypass | 4525232 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | 4530689 Security Update | Important | Security Feature Bypass | 4525236 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | 4530689 Security Update | Important | Security Feature Bypass | 4525236 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4530689 Security Update | Important | Security Feature Bypass | 4525236 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | 4530689 Security Update | Important | Security Feature Bypass | 4525236 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for 32-bit Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Security Feature Bypass | 4525235 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Security Feature Bypass | 4525235 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4530702 Monthly Rollup | Important | Security Feature Bypass | 4525243 | Base: 3.3<br>Temporal: 3 | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| | 4530730 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | |
| Windows 8.1 for x64-based systems | 4530702 Monthly Rollup 4530730 Security Only | Important | Security Feature Bypass | 4525243 | Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4530702 Monthly Rollup | Important | Security Feature Bypass | 4525243 | Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Security Feature Bypass | 4525234 | Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems | 4530695 Monthly Rollup 4530719 | Important | Security Feature Bypass | 4525234 | Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Security Only | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Security Feature Bypass | 4525234 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4530695 Monthly Rollup 4530719 Security Only | Important | Security Feature Bypass | 4525234 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems | 4530695 Monthly Rollup 4530719 Security | Important | Security Feature Bypass | 4525234 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Only | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Security Feature Bypass | 4525235 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4530734 Monthly Rollup 4530692 Security Only | Important | Security Feature Bypass | 4525235 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based | 4530734 Monthly Rollup 4530692 | Important | Security Feature Bypass | 4525235 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Security Only | | | | | |
| Windows Server 2012 | 4530691 Monthly Rollup 4530698 Security Only | Important | Security Feature Bypass | 4525246 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | 4530691 Monthly Rollup 4530698 Security Only | Important | Security Feature Bypass | 4525246 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | 4530702 Monthly Rollup 4530730 Security Only | Important | Security Feature Bypass | 4525243 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4530702 Monthly Rollup 4530730 Security Only | Important | Security Feature Bypass | 4525243 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for 32-bit Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for x64-based Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for ARM64-based Systems | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1909 | 4530684 Security Update | Important | Security Feature Bypass | 4524570 | Base: 3.3<br>Temporal: 3 | Yes |

| CVE-2019-1488 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C | |

# CVE-2019-1489 - Remote Desktop Protocol Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1489 MITRE NVD | **CVE Title:** Remote Desktop Protocol Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Windows Remote Desktop Protocol (RDP) fails to properly handle 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 attacker would have to connect remotely to an affected system and run a specially crafted application.<br><br>**FAQ:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Why is there no update for this vulnerability?**<br>Microsoft will not provide an update for this vulnerability because Windows XP is out of support. Microsoft strongly recommends upgrading to a supported version of Windows software.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1489 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Windows XP Service Pack 3 | | Important | Information Disclosure | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | |

# CVE-2019-1490 - Skype for Business Server Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2019-1490<br>MITRE<br>NVD | **CVE Title:** Skype for Business Server Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists when a Skype for Business Server does not properly sanitize a specially crafted request. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected server. The attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user.<br>For the vulnerability to be exploited, a user must click a specially crafted URL that takes the user to a targeted Skype for Business site. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user of the targeted Skype for Business site and convincing the user to click the specially crafted URL.<br><br>The security update addresses the vulnerability by helping to ensure that Skype for Business Server properly sanitizes web requests.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 12/10/2019 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2019-1490 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Skype for Business Server 2019 CU2 | 4534761 Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Yes |

## 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