# 微软发布 1 月补丁修复 49 个安全问题

## 安全威胁通告


发布时间：2020 年 1 月 15 日

# 综述

微软于周二发布了 1 月安全更新补丁，修复了 49 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.NET Framework、Apps、ASP.NET、Common Log File System Driver、Microsoft Dynamics、Microsoft Graphics Component、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows、Microsoft Windows Search Component、Windows Hyper-V、Windows Media、Windows RDP、Windows Subsystem for Linux 以及 Windows Update Stack。

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 8 个，分别存在于 .NET Framework、ASP.NET、Microsoft Scripting Engine 以及 Windows RDP 中。除此之外，还包含 41 个重要（Important）漏洞。

# Critical 漏洞概述

以下为此次更新中包含的 8 个 Critical 级别漏洞。

## Windows RDP

- **CVE-2020-0609、CVE-2020-0610**

  这两个 Windows 远程桌面网关（RD 网关）远程代码执行漏洞可被未经身份验证的攻击者利用。

  如果利用成功，则可能在目标系统上执行任意代码。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，攻击者将需要通过 RDP 向目标系统 RD 网关发送特制请求。

  本次更新通过更正 RD 网关处理连接请求的方式来解决该问题。

  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-2020-0609

  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610

- **CVE-2020-0611**

  这是 Windows 远程桌面客户端中的一个远程代码执行漏洞。

  成功利用此漏洞的攻击者可以在连接到恶意服务器的用户计算机上执行任意代码。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，攻击者需要控制服务器，然后诱使用户连接到该服务器。如果用户访问了恶意的服务器，则可以触发此漏洞。虽然攻击者无法强迫用户连接到恶意服务器，但他们可能会通过社工，DNS 中毒或中间人（MITM）技术诱使用户进行连接。攻击者还可能破坏合法服务器，在其上托管恶意代码，然后等待用户连接。

  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-2020-0611

## Microsoft Scripting Engine

- **CVE-2020-0640**

这是 Internet Explorer 处理内存中对象的方式中存在的一个内存损坏漏洞。该漏洞使攻击者可以在当前用户的上下文中执行任意代码。

成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，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。

攻击者可能会搭建一个特制的网站，然后诱使用户查看该网站。不过攻击者无法强迫用户查看恶意内容。所以通常会通过电子邮件或即时消息的方式来诱导用户。

Internet Explorer 9、10、11 均受影响。

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-2020-0640

## ASP.NET 和.NET Framework

- **CVE-2020-0603 、CVE-2020-0605、CVE-2020-0606、CVE-2020-0646**

以上漏洞是.NET 和 ASP.NET 核心软件中的远程代码执行漏洞。如果用户在使用受影响的.NET 或 ASP.NET Core 版本时打开恶意的特制文件，则可以触发这些漏洞。如果利用成功，攻击者便可以在当前用户的上下文中执行任意代码。这些错误存在于软件处理内存对象的方式中。

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-2020-0603

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0605

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0606
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646

# Important 漏洞概述

除了 Critical 漏洞外，此次更新还包含了 41 个 important 级别漏洞，其中 3 较需关注的漏洞如下。

## CVE-2020-0601

这是 Windows CryptoAPI 中的一个欺骗漏洞。由于 crypt32.dll 不正确地验证了椭圆曲线密码证书。攻击者可能利用此错误来欺骗代码签名证书并秘密签名文件，从而使该文件看起来好像来自受信任的源。攻击者也可能使用此漏洞进行中间人攻击并解密机密信息。

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-2020-0601

## CVE-2020-0616

这是一个 Microsoft Windows 拒绝服务漏洞。当 Windows 无法正确处理硬链接时，存在该漏洞。成功利用此漏洞的攻击者可能导致目标系统停止响应。

攻击者必须登录受害者计算机以利用此漏洞，然后运行经特殊设计的应用程序，该漏洞将使攻击者可以覆盖系统文件。

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-2020-0616

## CVE-2020-0654

Android 的 Microsoft OneDrive 应用程序中存在一个安全功能绕过漏洞。这可能使攻击者可以绕过应用程序的密码或指纹。
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-2020-0654

# 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 |
| --- | --- | --- | --- |
| .NET Framework | CVE-2020-0605 | .NET Framework 远程代码执行漏洞 | Critical |
| .NET Framework | CVE-2020-0606 | .NET Framework 远程代码执行漏洞 | Critical |
| .NET Framework | CVE-2020-0646 | .NET Framework Remote Code Execution Injection Vulnerability | Critical |

| | | | |
|---|---|---|---|
| Apps | CVE-2020-0654 | Microsoft OneDrive for Android 安全功能绕过漏洞 | Important |
| ASP.NET | CVE-2020-0602 | ASP.NET Core 拒绝服务漏洞 | Important |
| ASP.NET | CVE-2020-0603 | ASP.NET Core 远程代码执行漏洞 | Critical |
| Common Log File System Driver | CVE-2020-0615 | Windows Common Log File System Driver 信息泄露漏洞 | Important |
| Common Log File System Driver | CVE-2020-0639 | Windows Common Log File System Driver 信息泄露漏洞 | Important |
| Common Log File System Driver | CVE-2020-0634 | Windows Common Log File System Driver 特权提升漏洞 | Important |
| Microsoft Dynamics | CVE-2020-0656 | Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability | Important |
| Microsoft Graphics Component | CVE-2020-0607 | Microsoft Graphics Components 信息泄露漏洞 | Important |

| | | | |
|---|---|---|---|
| Microsoft Graphics Component | CVE-2020-0622 | Microsoft Graphics Component 信息泄露漏洞 | Important |
| Microsoft Graphics Component | CVE-2020-0642 | Win32k 特权提升漏洞 | Important |
| Microsoft Graphics Component | CVE-2020-0643 | Windows GDI+ 信息泄露漏洞 | Important |
| Microsoft Office | CVE-2020-0647 | Microsoft Office Online 欺骗漏洞 | Important |
| Microsoft Office | CVE-2020-0650 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2020-0651 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2020-0652 | Microsoft Office 内存破坏漏洞 | Important |
| Microsoft Office | CVE-2020-0653 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Scripting Engine | CVE-2020-0640 | Internet Explorer 内存破坏漏洞 | Critical |

| | | | |
|---|---|---|---|
| Microsoft Windows | CVE-2020-0601 | Windows CryptoAPI 欺骗漏洞 | Important |
| Microsoft Windows | CVE-2020-0608 | Win32k 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2020-0616 | Microsoft Windows 拒绝服务漏洞 | Important |
| Microsoft Windows | CVE-2020-0620 | Microsoft Cryptographic Services 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2020-0621 | Windows 安全功能绕过漏洞 | Important |
| Microsoft Windows | CVE-2020-0624 | Win32k 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2020-0635 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2020-0644 | Windows 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0613 | Windows Search Indexer 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| Microsoft Windows Search Component | CVE-2020-0614 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0623 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0625 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0626 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0627 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0628 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0629 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0630 | Windows Search Indexer 特权提升漏洞 | Important |

| | | | |
|---|---|---|---|
| Microsoft Windows Search Component | CVE-2020-0631 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0632 | Windows Search Indexer 特权提升漏洞 | Important |
| Microsoft Windows Search Component | CVE-2020-0633 | Windows Search Indexer 特权提升漏洞 | Important |
| Windows Hyper-V | CVE-2020-0617 | Hyper-V 拒绝服务漏洞 | Important |
| Windows Media | CVE-2020-0641 | Microsoft Windows 特权提升漏洞 | Important |
| Windows RDP | CVE-2020-0609 | Windows Remote Desktop Gateway (RD Gateway) 远程代码执行漏洞 | Critical |
| Windows RDP | CVE-2020-0610 | Windows Remote Desktop Gateway (RD Gateway) 远程代码执行漏洞 | Critical |

| | | | |
|---|---|---|---|
| **Windows RDP** | CVE-2020-0611 | Remote Desktop Client 远程代码执行漏洞 | Critical |
| **Windows RDP** | CVE-2020-0612 | Windows Remote Desktop Gateway (RD Gateway) 拒绝服务漏洞 | Important |
| **Windows RDP** | CVE-2020-0637 | Remote Desktop Web Access 信息泄露漏洞 | Important |
| **Windows Subsystem for Linux** | CVE-2020-0636 | Windows Subsystem for Linux 特权提升漏洞 | Important |
| **Windows Update Stack** | CVE-2020-0638 | Update Notification Manager 特权提升漏洞 | Important |

# 修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

# 附件

## CVE-2020-0601 - Windows CryptoAPI Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| CVE-2020-0601 MITRE NVD | **CVE Title:** Windows CryptoAPI Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates.<br><br>An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.<br><br>A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.<br><br>The security update addresses the vulnerability by ensuring that Windows CryptoAPI completely validates ECC certificates.<br><br>**FAQ:**<br>**Is there more information from Microsoft regarding CVE-2020-0601?**<br><br>Yes, please see the blog post release on 1/14/2020.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published.<br><br>1.1 01/14/2020 08:00:00 | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | Added an FAQ. This is an information change only. | | |

# Affected Software

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

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Spoofing | 4530717 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Spoofing | 4530717 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, | 4534293 Security | Important | Spoofing | 4530717 | Base: 8.1<br>Temporal: 7.3 | Unknown |

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| version 1803 (Server Core Installation) | Update | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Spoofing | 4530717 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Spoofing | 4530715 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Spoofing | 4530715 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Spoofing | 4530715 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security | Important | Spoofing | 4530715 | Base: 8.1<br>Temporal: 7.3 | Unknown |

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| | Update | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Spoofing | 4530715 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Spoofing | 4530714 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Spoofing | 4530714 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Spoofing | 4530714 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Spoofing | 4530681 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Spoofing | 4530681 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Spoofing | 4530689 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Spoofing | 4530689 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Spoofing | 4530689 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Spoofing | 4530689 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3 | Yes |

| CVE-2020-0601 | | | | | | |
|---|---|---|---|---|---|---|
| for x64-based Systems | | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | |
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Important | Spoofing | 4530684 | Base: 8.1<br>Temporal: 7.3<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0602 - ASP.NET Core Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0602 | **CVE Title:** ASP.NET Core Denial of Service Vulnerability<br>**Description:** | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| MITRE<br>NVD | A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication.<br><br>A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the ASP.NET Core application.<br><br>The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0602 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ASP.NET Core 2.1 | Release Notes Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| ASP.NET Core 3.0 | Release Notes Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| ASP.NET Core 3.1 | Rekease Notes Security Update | Important | Denial of Service | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0603 - ASP.NET Core Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0603<br>MITRE<br>NVD | **CVE Title:** ASP.NET Core Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in ASP.NET Core software when the software fails to handle objects in memory.<br><br>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 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 ASP.NET Core. 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.<br><br>The security update addresses the vulnerability by correcting how ASP.NET Core handles objects in memory. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0603 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0603 | | | | | | |
|---|---|---|---|---|---|---|
| ASP.NET Core 2.1 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| ASP.NET Core 3.0 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| ASP.NET Core 3.1 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0605 - .NET Framework Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0605<br>MITRE<br>NVD | **CVE Title:** .NET Framework Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file.<br><br>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 | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | attacker 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><br>Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of .NET Framework. 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.<br><br>The security update addresses the vulnerability by correcting how .NET Framework checks the source markup of a file.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| .NET Core 3.0 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| .NET Core 3.1 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1909 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534977 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation) | 4532936 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems | 4532936 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems | 4532935 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems | 4532936 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems | 4532935 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation) | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems | 4532933 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems | 4532933 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534978 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows Server 2016 | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534979 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.5.2 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 | 4535103 Monthly Rollup | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534977 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534976 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524744; 4533098 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A | Unknown |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

| CVE-2020-0605 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation) | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

# CVE-2020-0606 - .NET Framework Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0606<br>MITRE<br>NVD | **CVE Title:** .NET Framework Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file.<br><br>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 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 .NET Framework. 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.<br><br>The security update addresses the vulnerability by correcting how .NET Framework checks the source markup of a file. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| .NET Core 3.0 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| .NET Core 3.1 | Release Notes Security Update | Critical | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534978 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems | 4532936 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems | 4532936 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation) | 4532936 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems | 4532935 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems | 4532935 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2016 | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation) | 4532933 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534976 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534978 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A | Unknown |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4535102 Monthly Rollup | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534976 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534979 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1909 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation) | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A | Unknown |

| CVE-2020-0606 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

# CVE-2020-0607 - Microsoft Graphics Components Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020- | **CVE Title:** Microsoft Graphics Components Information Disclosure Vulnerability **Description:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| 0607<br>MITRE<br>NVD | An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information that could be useful for further exploitation.<br><br>To exploit the vulnerability, a user would have to open a specially crafted file.<br><br>The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64- | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version | 4534276 Security | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5 | Unknown |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| 1709 for ARM64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 (Server Core installation) | | | | | Vector: CVSS: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 for 32-bit Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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- | 4534310 Monthly Rollup | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 1 | 4534314 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 Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server | 4534283 Monthly Rollup | Important | Information Disclosure | 4530691 | Base: 5.5 Temporal: 5 | Unknown |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | 4534288 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 Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5 Temporal: 5 | Yes |

| CVE-2020-0607 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS: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 ARM64-based Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0608 - Win32k Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0608<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.<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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5 | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | Vector: CVSS: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 x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version | 4534271 Security | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5 | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| 1607 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 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534283 Monthly Rollup 4534288 | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0608 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | Vector: CVSS: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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0609 - Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0609<br>MITRE<br>NVD | **CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. 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 need to send a specially crafted request to the target systems RD Gateway via RDP.<br>The update addresses the vulnerability by correcting how RD Gateway handles connection requests. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0609 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0609 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Critical | Remote Code Execution | 4530691 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Critical | Remote Code Execution | 4530702 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

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

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0610 MITRE NVD | **CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. 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 need to send a specially crafted request to the target systems RD Gateway via RDP.<br>The update addresses the vulnerability by correcting how RD Gateway handles connection requests. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0610 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0610 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Critical | Remote Code Execution | 4530691 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Critical | Remote Code Execution | 4530702 | Base: 9.8<br>Temporal: 8.8<br>Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

# CVE-2020-0611 - Remote Desktop Client Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0611 MITRE NVD | **CVE Title:** Remote Desktop Client Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. 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 need to have control of a server and then convince a user to connect to it. An attacker would have no way of forcing a user to connect to the malicious server, they would need to trick the user into connecting via social engineering, DNS poisoning or using a Man in the Middle (MITM) technique. An attacker could also compromise a legitimate server, host malicious code on it, and wait for the user to connect.<br>The update addresses the vulnerability by correcting how the Windows Remote Desktop Client handles connection requests. | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Windows Server 2019 | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 |
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | 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 | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | 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 | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Critical | Remote Code Execution | 4530734 | 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 |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Critical | Remote Code Execution | 4530734 | 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 |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup | Critical | Remote Code Execution | 4530702 | Base: 7.5<br>Temporal: 6.7 | Unknown |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534309 Security Only | | | | 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 | |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Critical | Remote Code Execution | 4530702 | Base: 7.5 Temporal: 6.7 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 | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Critical | Remote Code Execution | 4530702 | Base: 7.5 Temporal: 6.7 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 | Unknown |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Critical | Remote Code Execution | 4530734 | Base: 7.5 Temporal: 6.7 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-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Critical | Remote Code Execution | 4530734 | 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 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Critical | Remote Code Execution | 4530734 | 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 |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Critical | Remote Code Execution | 4530691 | 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 | Unknown |

| CVE-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Critical | Remote Code Execution | 4530691 | 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 | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Critical | Remote Code Execution | 4530702 | 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 | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Critical | Remote Code Execution | 4530702 | 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 | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0611 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 |
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 |
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0612 - Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0612 MITRE NVD | **CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) 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 RD Gateway 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 RD Gateway services.<br>The update addresses the vulnerability by correcting how RD Gateway 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0612 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2019 | 4534273 Security Update | Important | Denial of Service | 4530715 | 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 | Unknown |

| CVE-2020-0612 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Denial of Service | 4530689 | 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 | Unknown |

# CVE-2020-0613 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0613<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly handles objects in memory. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64- | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64- | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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- | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0613 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0614 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0614 | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| MITRE<br>NVD | An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br><br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br><br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0614 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0615 - Windows Common Log File System Driver Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0615<br>MITRE<br>NVD | **CVE Title:** Windows Common Log File System Driver Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.<br>To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.<br>The security update addresses the vulnerability by correcting how CLFS handles objects in memory.<br><br>**FAQ:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | **What type of information could be disclosed by this vulnerability?**<br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64- | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version | 4528760 Security | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Pack 2 (Server Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Security Only | | | | | |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0615 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0616 - Microsoft Windows Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0616 MITRE NVD | **CVE Title:** Microsoft Windows Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Windows improperly handles hard links. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.<br>To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would allow an attacker to overwrite system files. | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses the vulnerability by correcting ACLs to system files.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0616 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0616 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0616 | | | | | | |
|---|---|---|---|---|---|---|
| for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0616 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Important | Denial of Service | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0617 - Hyper-V Denial of Service Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0617 MITRE NVD | **CVE Title:** Hyper-V Denial of Service Vulnerability<br>**Description:**<br>A denial of service vulnerability exists when Microsoft Hyper-V Virtual PCI on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating | Important | Denial of Service |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash.<br><br>To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.<br><br>The security update addresses the vulnerability by properly validating input.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0617 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Denial of Service | 4530717 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Denial of Service | 4530717 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.3<br>Temporal: 4.8 | Unknown |

| CVE-2020-0617 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Denial of Service | 4530715 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Denial of Service | 4530714 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Denial of Service | 4530681 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Denial of Service | 4530689 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Denial of Service | 4530689 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0617 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Denial of Service | 4530689 | Base: 5.3<br>Temporal: 4.8<br>Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Unknown |

# CVE-2020-0620 - Microsoft Cryptographic Services Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0620 MITRE NVD | **CVE Title:** Microsoft Cryptographic Services Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when Microsoft Cryptographic Services improperly handles files. An attacker could exploit the vulnerability to overwrite or modify a protected file leading to a privilege escalation.<br>To exploit the vulnerability, an attacker would first require execution on the victim system.<br>The security update addresses the vulnerability by addressing how Microsoft Cryptographic Services handles files. | 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534309 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Security Only | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| 1 (Server Core installation) | | | | | | |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0620 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |

# CVE-2020-0621 - Windows Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0621<br>MITRE<br>NVD | **CVE Title:** Windows Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists in Windows 10 when third party filters are called during a password update. Successful exploitation of the vulnerability could allow a user to make use of a blocked password for their account.<br>To exploit the vulnerability, an attacker would need have access and the current password for the target user.<br>The update addresses how password filters are called during a password update.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0621 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Security Feature Bypass | 4530717 | Base: 4.4<br>Temporal: 4<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 | 4534293 Security Update | Important | Security Feature Bypass | 4530717 | Base: 4.4<br>Temporal: 4 | Unknown |

| CVE-2020-0621 | | | | | | |
|---|---|---|---|---|---|---|
| for x64-based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Security Feature Bypass | 4530717 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Security Feature Bypass | 4530717 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Security Feature Bypass | 4530715 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Security Feature Bypass | 4530715 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64- | 4534273 Security Update | Important | Security Feature Bypass | 4530715 | Base: 4.4<br>Temporal: 4 | Unknown |

| CVE-2020-0621 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | |
| Windows Server 2019 | 4534273 Security Update | Important | Security Feature Bypass | 4530715 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Security Feature Bypass | 4530715 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Security Feature Bypass | 4530714 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Security Feature Bypass | 4530714 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64- | 4534276 Security Update | Important | Security Feature Bypass | 4530714 | Base: 4.4<br>Temporal: 4<br>Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0621 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |

# CVE-2020-0622 - Microsoft Graphics Component Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0622 MITRE NVD | **CVE Title:** Microsoft Graphics Component Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the 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.<br>The update addresses the vulnerability by correcting the way in which the Windows Graphics 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0622 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64- | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0622 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64- | 4534306 Security | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5 | Unknown |

| CVE-2020-0622 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

# CVE-2020-0623 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0623<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64- | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534309 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0623 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0624 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0624 MITRE NVD | **CVE Title:** Win32k Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0624 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0624 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0624 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0625 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0625<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0625 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0626 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0626<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0626 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0627 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0627<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0627 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0628 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0628<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0628 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0629 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0629<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0629 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0630 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0630<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0630 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0631 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0631<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0631 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0632 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0632<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems | 4534310 Monthly Rollup | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | 4534314 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 7 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems | 4534303 Monthly Rollup 4534312 Security | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | Only | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 1 | | | | | | |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0632 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0633 - Windows Search Indexer Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0633<br>MITRE<br>NVD | **CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.<br>To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.<br>The security update addresses the vulnerability by ensuring the Windows Search Indexer properly 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64- | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0633 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1909 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0634 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0634 MITRE NVD | **CVE Title:** Windows Common Log File System Driver Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.<br><br>The security update addresses the vulnerability by correcting how CLFS handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534309 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Security Only | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| 1 (Server Core installation) | | | | | | |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0634 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |

# CVE-2020-0635 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0635 MITRE NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links. An attacker who successfully exploited this vulnerability could potentially set certain items to run at a higher level and thereby elevate permissions.<br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br>The update addresses this vulnerability by correcting how the Windows handles symbolic 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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534309 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 | Important | Elevation of Privilege | 4530695 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 (Server Core installation) | Security Only | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| 1 (Server Core installation) | | | | | | |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0635 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |

# CVE-2020-0636 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0636 MITRE NVD | **CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files. An attacker who successfully exploited the vulnerability could execute code with elevated privileges.<br>To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application.<br>The security update addresses the vulnerability by correcting how the Windows Subsystem for Linux handles files.<br><br>**FAQ:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0636 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0636 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0636 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0637 - Remote Desktop Web Access Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0637 MITRE NVD | **CVE Title:** Remote Desktop Web Access Information Disclosure Vulnerability<br>**Description:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | An information disclosure vulnerability exists when Remote Desktop Web Access improperly handles credential information. An attacker who successfully exploited this vulnerability could obtain legitimate users' credentials.<br><br>To exploit this vulnerability, an attacker would need access to a vulnerable server with the Remote Desktop Web Access role.<br><br>The security update addresses the vulnerability by correcting how Remote Desktop Web Access handles credential information.<br><br>**FAQ:**<br>**What type of information could be disclosed by this vulnerability?**<br><br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is sensitive information.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0637 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.7<br>Temporal: 5.1<br>Vector:<br>CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.7<br>Temporal: 5.1<br>Vector:<br>CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.7<br>Temporal: 5.1<br>Vector:<br>CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.7<br>Temporal: 5.1 | Unknown |

| CVE-2020-0637 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 | Important | Information Disclosure | 4530691 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0637 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.7<br>Temporal: 5.1<br>Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

# CVE-2020-0638 - Update Notification Manager Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0638<br>MITRE<br>NVD | **CVE Title:** Update Notification Manager Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists in the way the Update Notification Manager handles files.<br><br>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 the Update Notification Manager handles files.<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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0638 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0638 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0638 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0638 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1903 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0638 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0639 - Windows Common Log File System Driver Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0639<br>MITRE<br>NVD | **CVE Title:** Windows Common Log File System Driver Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.<br>To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.<br>The security update addresses the vulnerability by correcting how CLFS handles objects in memory.<br><br>**FAQ:** | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | **What type of information could be disclosed by this vulnerability?**<br>The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64- | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version | 4528760 Security | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 for 32-bit Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | | | | | | |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Pack 2 (Server Core installation) | | | | | | |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 (Server Core installation) | Security Only | | | | | |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0639 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server, version 1909 (Server Core installation) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0640 - Internet Explorer Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0640 MITRE NVD | **CVE Title:** Internet Explorer Memory Corruption Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker could take control of an affected | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.<br><br>The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 10 on Windows Server 2012 | 4534283 Monthly Rollup 4534251 IE Cumulative | Moderate | Remote Code Execution | 4530677 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534251 IE Cumulative 4534303 Monthly Rollup | Moderate | Remote Code Execution | 4530695 | 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 | 4534251 IE Cumulative 4534303 Monthly Rollup | Moderate | Remote Code Execution | 4530695 | 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 | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: 7.5<br>Temporal: 6.7 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for 32-bit Systems | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64- | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | 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 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | 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 | Unknown |
| Internet Explorer 11 on | 4534273 Security Update | Critical | Remote Code Execution | 4530715 | Base: 7.5<br>Temporal: 6.7 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | | | | | Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Internet Explorer 11 on Windows Server 2019 | 4534273 Security Update | Moderate | Remote Code Execution | 4530715 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | 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 | Unknown |
| Internet Explorer 11 on Windows | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| 10 Version 1903 for 32-bit Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 ARM64- | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 for x64-based Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1607 for | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| 32-bit Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | 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 | Unknown |
| Internet Explorer 11 on Windows Server 2016 | 4534271 Security Update | Moderate | Remote Code Execution | 4530689 | 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 | Unknown |
| Internet Explorer 11 on Windows 7 for 32-bit | 4534251 IE Cumulative 4534310 Monthly Rollup | Critical | Remote Code Execution | 4530734 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Systems Service Pack 1 | | | | | | |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | 4534251 IE Cumulative 4534310 Monthly Rollup | Critical | Remote Code Execution | 4530734 | 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 32-bit systems | 4534251 IE Cumulative 4534297 Monthly Rollup | Critical | Remote Code Execution | 4530702 | 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 | Unknown |
| Internet Explorer 11 on Windows | 4534251 IE Cumulative 4534297 Monthly | Critical | Remote Code Execution | 4530702 | 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 | Unknown |

| CVE-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| 8.1 for x64-based systems | Rollup | | | | | |
| Internet Explorer 11 on Windows RT 8.1 | 4534297 Monthly Rollup | Critical | Remote Code Execution | 4530702 | 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 | Unknown |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4534251 IE Cumulative 4534310 Monthly Rollup | Moderate | Remote Code Execution | 4530734 | 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 | 4534251 IE Cumulative | Moderate | Remote Code Execution | 4530677 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| Server 2012 | | | | | | |
| Internet Explorer 11 on Windows Server 2012 R2 | 4534251 IE Cumulative 4534297 Monthly Rollup | Moderate | Remote Code Execution | 4530702 | 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 | Unknown |
| Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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 | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0640 | | | | | | |
|---|---|---|---|---|---|---|
| 1909 for x64-based Systems | | | | | | |
| Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Critical | Remote Code Execution | 4530684 | 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-2020-0641 - Microsoft Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0641 | **CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability<br>**Description:** | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| MITRE<br>NVD | An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.<br><br>To exploit the 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 the vulnerability by correcting how the Windows Media Service handles file creation.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for x64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0641 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0642 - Win32k Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0642 MITRE 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 | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br><br>To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.<br><br>The update addresses this vulnerability by correcting how Win32k handles objects in memory.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64- | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Elevation of Privilege | 4530695 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Elevation of Privilege | 4530734 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64- | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7 | Yes |

| CVE-2020-0642 | | | | | | |
|---|---|---|---|---|---|---|
| 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 1909 (Server Core installation) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0643 - Windows GDI+ Information Disclosure Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0643 MITRE NVD | **CVE Title:** Windows GDI+ Information Disclosure Vulnerability<br>**Description:**<br>An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. | Important | Information Disclosure |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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 GDI+ handles memory addresses.<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 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server, version 1803 (Server | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Core Installation) | | | | | | |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Information Disclosure | 4530717 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for ARM64- | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server 2019 | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Information Disclosure | 4530715 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version | 4534276 Security | Important | Information Disclosure | 4530714 | Base: 5.5<br>Temporal: 5 | Unknown |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| 1709 for ARM64-based Systems | Update | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| 1903 (Server Core installation) | | | | | Vector: CVSS: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 for 32-bit Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Information Disclosure | 4530681 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Information Disclosure | 4530689 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 7 for 32-bit Systems Service Pack 1 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Information Disclosure | 4530702 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Service Pack 2 | | | | | | |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | 4534303 Monthly Rollup 4534312 Security Only | Important | Information Disclosure | 4530695 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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 | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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- | 4534310 Monthly Rollup | Important | Information Disclosure | 4530734 | Base: 5.5<br>Temporal: 5 | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems Service Pack 1 | 4534314 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 Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4534310 Monthly Rollup 4534314 Security Only | Important | Information Disclosure | 4530734 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 | 4534283 Monthly Rollup 4534288 Security Only | Important | Information Disclosure | 4530691 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 (Server | 4534283 Monthly Rollup | Important | Information Disclosure | 4530691 | Base: 5.5 Temporal: 5 | Unknown |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| Core installation) | 4534288 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 Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Information Disclosure | 4530702 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5 Temporal: 5 | Yes |

| CVE-2020-0643 | | | | | | |
|---|---|---|---|---|---|---|
| x64-based Systems | | | | | Vector: CVSS: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 ARM64-based Systems | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Information Disclosure | 4530684 | Base: 5.5<br>Temporal: 5<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2020-0644 - Windows Elevation of Privilege Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0644<br>MITRE<br>NVD | **CVE Title:** Windows Elevation of Privilege Vulnerability<br>**Description:**<br>An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names. An attacker who successfully exploited this vulnerability could run arbitrary code as system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.<br>To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application designed to elevate privileges.<br>The update addresses the vulnerability by correcting how Windows assigns memory to specific processes.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | Important | Elevation of Privilege |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for x64- | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector:<br>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| based Systems | | | | | | |
| Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1803 for ARM64-based Systems | 4534293 Security Update | Important | Elevation of Privilege | 4530717 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for 32-bit Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1809 for x64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1809 for ARM64-based Systems | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2019 (Server Core installation) | 4534273 Security Update | Important | Elevation of Privilege | 4530715 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1709 for ARM64-based Systems | 4534276 Security Update | Important | Elevation of Privilege | 4530714 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1903 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1903 for ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| (Server Core installation) | | | | | | |
| Windows 10 for 32-bit Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 for x64-based Systems | 4534306 Security Update | Important | Elevation of Privilege | 4530681 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2016 | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| Windows Server 2016 (Server Core installation) | 4534271 Security Update | Important | Elevation of Privilege | 4530689 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for 32-bit systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows 8.1 for x64-based systems | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows RT 8.1 | 4534297 Monthly Rollup | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 | 4534283 Monthly Rollup | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7 | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534288 Security Only | | | | Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | |
| Windows Server 2012 (Server Core installation) | 4534283 Monthly Rollup 4534288 Security Only | Important | Elevation of Privilege | 4530691 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |
| Windows Server 2012 R2 (Server Core installation) | 4534297 Monthly Rollup 4534309 Security Only | Important | Elevation of Privilege | 4530702 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Unknown |

| CVE-2020-0644 | | | | | | |
|---|---|---|---|---|---|---|
| Windows 10 Version 1909 for 32-bit Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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 ARM64-based Systems | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/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) | 4528760 Security Update | Important | Elevation of Privilege | 4530684 | Base: 7.8<br>Temporal: 7<br>Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2020-0646 - .NET Framework Remote Code Execution Injection Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0646<br>MITRE<br>NVD | **CVE Title:** .NET Framework Remote Code Execution Injection Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. 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 need to pass specific input to an application utilizing susceptible .Net methods.<br>The security update addresses the vulnerability by correcting how the Microsoft .NET Framework validates input.<br><br>**FAQ:** | Critical | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534976 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1 | 4535104 Monthly | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup 4534977 Security Only | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems | 4532936 Security | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Update | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems | 4532936 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation) | 4532936 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems | 4532935 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems | 4532935 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems | 4532933 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems | 4532933 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2016 | 4532933 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation) | 4532933 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534976 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows RT 8.1 | 4535104 Monthly | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation) | 4535103 Monthly | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup 4534977 Security Only | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Update | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation) | 4535101 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2 | 4535105 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534979 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | 4534978 Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Rollup 4534978 Security Only | | | | N/A Vector: N/A | |
| Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows RT 8.1 | 4535104 Monthly Rollup | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Only | | | | | |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2 | 4535105 Monthly Rollup 4534979 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | 4535102 Monthly Rollup 4534976 Security Only | Critical | Remote Code Execution | 4524741; 4533095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 | 4535103 Monthly Rollup 4534977 | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | Security Only | | | | Vector: N/A | |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation) | 4535103 Monthly Rollup 4534977 Security Only | Critical | Remote Code Execution | 4524742; 4533096 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation) | 4535104 Monthly Rollup 4534978 Security Only | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A | Maybe |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1909 (Server Core installation) | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for x64-based Systems | 4532938 Security Update | Critical | Remote Code Execution | 4524743; 4533097 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation) | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems | 4534293 Security Update | Critical | Remote Code Execution | 4530717 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation) | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems | 4534306 Security Update | Critical | Remote Code Execution | 4530681 | Base: N/A Temporal: N/A | Unknown |

| CVE-2020-0646 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Vector: N/A | |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems | 4534276 Security Update | Critical | Remote Code Execution | 4530714 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 | 4534271 Security Update | Critical | Remote Code Execution | 4530689 | Base: N/A Temporal: N/A Vector: N/A | Unknown |

# CVE-2020-0647 - Microsoft Office Online Spoofing Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0647<br>MITRE<br>NVD | **CVE Title:** Microsoft Office Online Spoofing Vulnerability<br>**Description:**<br>A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications correctly. An attacker could exploit the vulnerability by sending a specially crafted request to an affected site.<br><br>The attacker who successfully exploited the vulnerability could then perform cross-origin attacks on affected systems. These attacks could allow the attacker to read content that the attacker is not authorized to read, and use the victim's identity to take actions on the site on behalf of the victim. The victim needs to be authenticated for an attacker to compromise the victim.<br><br>The security update addresses the vulnerability by ensuring that Office Online properly validates origins.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector. | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0647 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Office Online Server | 4484223 Security Update | Important | Spoofing | 4484141 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0650 - Microsoft Excel Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0650<br>MITRE<br>NVD | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.<br><br>Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.<br><br>The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0650 | | | | | | |
|---|---|---|---|---|---|---|
| **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: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |

| CVE-2020-0650 | | | | | | |
|---|---|---|---|---|---|---|
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2016 (32-bit edition) | 4484217 Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | 4484217 Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | 4484243 Security Update | Important | Remote Code Execution | 4484196 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | 4484243 Security Update | Important | Remote Code Execution | 4484196 | Base: N/A Temporal: | Maybe |

| CVE-2020-0650 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Excel 2013 RT Service Pack 1 | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0651 - Microsoft Excel Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0651 MITRE NVD | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.<br><br>Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.<br><br>The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0651 | | | | | | |
|---|---|---|---|---|---|---|
| **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: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac | Release Notes Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |

| CVE-2020-0651 | | | | | | |
|---|---|---|---|---|---|---|
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2016 (32-bit edition) | 4484217 Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | 4484217 Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | Release Notes Security Update | Important | Remote Code Execution | 4484179 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | 4484243 Security Update | Important | Remote Code Execution | 4484196 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | 4484243 Security Update | Important | Remote Code Execution | 4484196 | Base: N/A Temporal: | Maybe |

| CVE-2020-0651 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Excel 2013 RT Service Pack 1 | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | 4484234 Security Update | Important | Remote Code Execution | 4484190 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0652 - Microsoft Office Memory Corruption Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0652<br>MITRE<br>NVD | **CVE Title:** Microsoft Office Memory Corruption Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Office 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 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 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 | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | 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.<br><br>The security update addresses the vulnerability by correcting how Office 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:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0652 | | | | | | |
|---|---|---|---|---|---|---|
| **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: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | | Base: N/A Temporal: N/A Vector: N/A | No |

| CVE-2020-0652 | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft Office 2016 (32-bit edition) | 4484221 Security Update | Important | Remote Code Execution | 4484182 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | 4484221 Security Update | Important | Remote Code Execution | 4484182 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | 4484236 Security Update | Important | Remote Code Execution | 4484192 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | 4484236 Security Update | Important | Remote Code Execution | 4484192 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4484227 Security Update | Important | Remote Code Execution | 4484184 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | 4484227 Security Update | Important | Remote Code Execution | 4484184 | Base: N/A Temporal: | Maybe |

| CVE-2020-0652 | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | N/A<br>Vector: N/A | |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | 4484227 Security Update | Important | Remote Code Execution | 4484184 | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0653 - Microsoft Excel Remote Code Execution Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0653<br>MITRE<br>NVD | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability<br>**Description:**<br>A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take 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. | Important | Remote Code Execution |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
| --- | --- | --- | --- |
| | Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.<br><br>The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.<br><br>**FAQ:**<br>**Is the Preview Pane an attack vector for this vulnerability?**<br><br>No, the Preview Pane is not an attack vector.<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None | | |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0653 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| 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 | No |
| 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 | No |

# CVE-2020-0654 - Microsoft OneDrive for Android Security Feature Bypass Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0654<br>MITRE<br>NVD | **CVE Title:** Microsoft OneDrive for Android Security Feature Bypass Vulnerability<br>**Description:**<br>A security feature bypass vulnerability exists in Microsoft OneDrive App for Android.<br>This could allow an attacker to bypass the passcode or fingerprint requirements of the App.<br>The security update addresses the vulnerability by correcting the way Microsoft OneDrive App for Android handles sharing links.<br><br>**FAQ:**<br>**How do I get the update for OneDrive for Android?**<br>1. Tap the **Google Play** icon on your home screen.<br>2. Swipe in from the left edge of the screen.<br>3. Tap **My apps & games**.<br>4. Tap the Update box next to the **OneDrive app**. | Important | Security Feature Bypass |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | **Is there a direct link on the web?**<br>Yes: https://play.google.com/store/apps/details?id=com.microsoft.skydrive&hl=en_US<br><br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0654 | | | | | | |
|---|---|---|---|---|---|---|
| Product | KB Article | Severity | Impact | Supersedence | CVSS Score Set | Restart Required |

| CVE-2020-0654 | | | | | | |
|---|---|---|---|---|---|---|
| One Drive for Android | Release Notes Security Update | Important | Security Feature Bypass | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

# CVE-2020-0656 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| CVE-2020-0656<br>MITRE<br>NVD | **CVE Title:** Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability<br>**Description:**<br>A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server.<br>The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on | Important | Spoofing |

| CVE ID | Vulnerability Description | Maximum Severity Rating | Vulnerability Impact |
|---|---|---|---|
| | behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.<br><br>The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.<br><br>**FAQ:**<br>None<br>**Mitigations:**<br>None<br>**Workarounds:**<br>None<br>**Revision:**<br>1.0 01/14/2020 08:00:00<br>Information published. | | |

# Affected Software

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

| CVE-2020-0656 | | | | | | |
|---|---|---|---|---|---|---|
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Dynamics 365 Field Service (on-premises) v7 series | Relelase Notes Security Update | Important | Spoofing | | Base: N/A<br>Temporal: N/A<br>Vector: N/A | Maybe |

## 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