
# گزارش اصلاحیه امنیتی مایکروسافت در ماه فوریه ۲۰۲۰

مایکروسافت آخرین به‌روزرسانی را برای آسیب‌پذیری‌های نرم افزارها و سیستم‌عامل‌های این شرکت منتشر کرده است. مرکز پاسخگویی امنیتی مایکروسافت (MSRC) تمام گزارش‌های آسیب‌پذیری‌های امنیتی موثر بر محصولات و خدمات مایکروسافت را بررسی می‌کند و اطلاعات را به عنوان بخشی از تلاش‌های مداوم برای کمک به مدیریت خطرات امنیتی و کمک به حفاظت از سیستم‌های کاربران فراهم می‌نماید. MSRC همراه با همکاران خود و محققان امنیتی در سراسر جهان برای کمک به پیشگیری از وقایع امنیتی و پیشبرد امنیت مایکروسافت فعالیت می‌کند.

به‌روزرسانی امنیتی در **ماه فوریه سال ۲۰۲۰** شامل موارد زیر برای محصولات مایکروسافت در درجه حساسیت بحرانی[1] و مهم[2] بوده است.

- **Microsoft Edge (Edge HTML - based)**
- **Internet Explorer**
- **Windows**
- **Chakra Core**

وصله امنیتی هر کدام از آسیب‌پذیری‌ها بر اساس نسخه خاصی از سیستم‌عامل نوشته شده است. کاربر می‌بایست با استفاده از فرمان winver در CMD نسخه سیستم‌عامل خود را بدست آورد سپس وصله امنیتی مورد نظر خود را دانلود نماید.

[1] Critical
2 Important

| | |
|---|---|
| نام محصول | Chakra Core<br>Microsoft Edge (Edge HTML - based), Internet Explorer |
| نام آسیب‌پذیری | Chakra Scripting Engine Memory Corruption Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-2020-0673<br>CVE-2020-0674<br>CVE-2020-0767<br>CVE-2020-0710<br>CVE-2020-0712<br>CVE-2020-0711<br>CVE-2020-0713 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 02/11/2020 |
| سیستم‌عامل | Windows Server 2012<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1803 for ARM64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows Server 2019<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1709 for ARM64-based Systems<br>Windows 10 Version 1903 for 32-bit Systems<br>Windows 10 Version 1903 for x64-based Systems<br>Windows 10 Version 1903 for ARM64-based Systems<br>Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows Server 2016<br>Windows 7 for 32-bit Systems Service Pack 1<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows 8.1 for 32-bit systems<br>Windows 8.1 for x64-based systems<br>Windows RT 8.1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2012 |

| | |
|---|---|
| | Windows Server 2012 R2<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for x64-based Systems Service Pack 2 |
| **توضیحات** | یک آسیب‌پذیری اجرای کد از راه دور موجود در موتور اسکریپت چاکرا بر روی Microsoft Edge وجود دارد که در هنگام مدیریت اشیاء بر روی مموری ایجاد می‌شود. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کد دلخواه را در زمینه کاربر فعلی اجرا کند. یک مهاجم که با موفقیت آسیب‌پذیری را مورد سوءاستفاده قرار دهد، قادر است همان دسترسی کاربر فعلی را بدست آورد و سیستم آسیب دیده را کنترل کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت‌های زیر را خواهد داشت.<br>• برنامه ها را نصب و یا حذف کند<br>• می تواند به مشاهده، تغییر یا حذف داده ها بپردازد.<br>• حساب کاربری جدید با حقوق کامل برای خود بسازد.<br>• یک در پشتی ایجاد کند و ... |
| **رفع آسیب‌پذیری** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0713<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0711<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0712<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0710<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0767<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0673 |

| نام محصول | windows |
|---|---|
| نام آسیب‌پذیری | Microsoft Windows Media Foundation Remote Code Execution Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-2020-0738 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 02/11/2020 |
| سیستم‌عامل | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for ARM64-based Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 Version 1803 for ARM64-based Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1903 for 32-bit Systems<br>Windows 10 Version 1903 for ARM64-based Systems<br>Windows 10 Version 1903 for x64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 7 for 32-bit Systems Service Pack 1<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows 8.1 for 32-bit systems<br>Windows 8.1 for x64-based systems<br>Windows RT 8.1<br>Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation) |

| | |
|---|---|
| | Windows Server, version 1803 (Server Core Installation)<br>Windows Server, version 1903 (Server Core installation)<br>Windows Server, version 1909 (Server Core installation) |
| توضیحات | آسیب‌پذیری اجرای کد از راه دور هنگامی که Windows Media Foundation به طور نامناسب فایل‌های QuickTime media دستکاری شده را تجزیه و تحلیل کند، وجود دارد. مهاجمی که از این آسیب‌پذیری بهره‌برداری کند، می‌تواند دسترسی کاربر محلی را به‌دست آورد. |
| رفع آسیب‌پذیری | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0738 |

| | |
|---|---|
| نام محصول | **Windows** |
| نام آسیب‌پذیری | **LNK Remote Code Execution Vulnerability** |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-2020-0729 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 02/11/2020 |
| سیستم‌عامل | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for ARM64-based Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 Version 1803 for ARM64-based Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1903 for 32-bit Systems<br>Windows 10 Version 1903 for ARM64-based Systems<br>Windows 10 Version 1903 for x64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 7 for 32-bit Systems Service Pack 1 |

| | |
|---|---|
| Windows 7 for x64-based Systems Service Pack 1<br>Windows 8.1 for 32-bit systems<br>Windows 8.1 for x64-based systems<br>Windows RT 8.1<br>Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server, version 1803 (Server Core Installation)<br>Windows Server, version 1903 (Server Core installation)<br>Windows Server, version 1909 (Server Core installation) | |
| یک آسیب‌پذیری در ویندوز وجود دارد که در صورت پردازش یک فایل LNK.، امکان اجرای کد از راه دور ایجاد می‌شود. مهاجمی که از این آسیب‌پذیری بهره‌برداری کند، می‌تواند دسترسی کاربر محلی را به‌دست آورد. | **توضیحات** |
| https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0729 | **رفع آسیب‌پذیری** |

| | |
|---|---|
| نام محصول | Windows |
| نام آسیب‌پذیری | Remote Desktop Client Remote Code Execution Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-2020-0817<br>CVE-2020-0734<br>CVE-2020-0681 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 09/10/2019 |
| سیستم‌عامل | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for ARM64-based Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 Version 1803 for ARM64-based Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1903 for 32-bit Systems<br>Windows 10 Version 1903 for ARM64-based Systems<br>Windows 10 Version 1903 for x64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 7 for 32-bit Systems Service Pack 1<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows 8.1 for 32-bit systems<br>Windows 8.1 for x64-based systems<br>Windows RT 8.1<br>Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation) |

| | |
|---|---|
| | Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server, version 1803 (Server Core Installation)<br>Windows Server, version 1903 (Server Core installation)<br>Windows Server, version 1909 (Server Core installation) |
| توضیحات | یک آسیب‌پذیری اجرای کد از راه دور موجود در Remote Desktop client، زمانی که یک کاربر از طریق RDP به سرور آلوده متصل می‌شود، وجود دارد. یک مهاجم که با موفقیت آسیب‌پذیری را مورد سوءاستفاده قرار داده است، توانایی فعالیت‌های زیر را خواهد داشت.<br>• برنامه ها را نصب و یا حذف کند<br>• می تواند به مشاهده، تغییر یا حذف داده ها بپردازد.<br>• حساب کاربری جدید با حقوق کامل برای خود بسازد.<br>• یک در پشتی ایجاد کند و ... |
| رفع آسیب‌پذیری | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0817<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0734<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0681 |

| | |
|---|---|
| نام محصول | **Windows** |
| نام آسیب‌پذیری | **Internet Connection Sharing Service Remote Code Execution Vulnerability** |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-2020-0662 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 02/11/2020 |
| سیستم‌عامل | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for ARM64-based Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 Version 1803 for ARM64-based Systems<br>Windows 10 Version 1803 for x64-based Systems |

| | |
|---|---|
| Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1903 for 32-bit Systems<br>Windows 10 Version 1903 for ARM64-based Systems<br>Windows 10 Version 1903 for x64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 7 for 32-bit Systems Service Pack 1<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows 8.1 for 32-bit systems<br>Windows 8.1 for x64-based systems<br>Windows RT 8.1<br>Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server, version 1803 (Server Core Installation)<br>Windows Server, version 1903 (Server Core installation)<br>Windows Server, version 1909 (Server Core installation) | |
| آسیب‌پذیری حافظه موجود در سرویس اتصال به اینترنت (ICS) هنگامی که یک مهاجم بسته‌های دستکاری شده ویژه را به سرور ارسال می‌کند، وجود دارد. مهاجمی که با موفقیت از آسیب‌پذیری بهره‌برداری کند، می‌تواند کد دلخواه خود را بر روی سرور اجرا کند. | **توضیحات** |
| https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0662 | **رفع آسیب‌پذیری** |

| | |
|---|---|
| نام محصول | **Microsoft SQL Server** |
| نام آسیب‌پذیری | **Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability** |
| حساسیت | Important |
| شناسه آسیب‌پذیری | CVE-2020-0618 |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | 11/12/2019 |
| محصولات | Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU)<br>Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)<br>Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU)<br>Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)<br>Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU)<br>Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR) |
| توضیحات | آسیب‌پذیری اجرای کد از راه دور در سرویس‌های گزارش دهی **Microsoft SQL Server** هنگامی که به طور نادرست به درخواست‌های صفحه پاسخ می‌دهد، ایجاد می‌شود. مهاجمی که با موفقیت از این آسیب‌پذیری استفاده کرده است می‌تواند در سرویس گزارش کد دلخواه را اجرا کند. |
| رفع آسیب‌پذیری | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618 |