
# گزارش اصلاحیه امنیتی مایکروسافت در ماه اکتبر ۲۰۱۸

مایکروسافت به‌روزرسانی‌هایی برای آسیب‌پذیری در نرم‌افزارهای مایکروسافت را منتشر کرده است. مهاجم از راه دور می تواند از برخی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب دیده استفاده کند.

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 اکتبر سال ۲۰۱۸ برای محصولات در درجه حساسیت بحرانی[۱] به صورت زیر بوده است:

- ChakraCore
- Microsoft Edge
- Internet Explorer
- Windows

همچنین مایکروسافت در لینک‌های زیر توصیه‌های امنیتی و توضیحاتی بیشتر را داشته است که مطالعه آن بسیار مفید خواهد بود.

https://portal.msrc.microsoft.com/en-us/security-guidance

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/aa۹۹ba۲۸-e۹۹f-e۸۱۱-a۹۷۸-۰۰۰d۳a۳۳c۵۷۳۳

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

لیست آسیب پذیری‌های جدید بر اساس محصولات و درجه حساسیت بحرانی در ادامه شرح داده خواهند شد.

[۱] Critical

| | |
|---|---|
| نام محصول | Chakra Core |
| نام آسیب‌پذیری | Chakra Scripting Engine Memory Corruption Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۵۰۵<br>CVE-۲۰۱۸-۸۵۱۰<br>CVE-۲۰۱۸-۸۵۱۱<br>CVE-۲۰۱۸-۸۵۱۳ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | ۲۰۱۸/۱۰/۹ |
| سیستم‌عامل | Windows Server 2016<br>Windows 10 Version 1703 for x64-based Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows Server 2012 R2<br>Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1703 for 32-bit Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems |
| توضیحات | آسیب پذیری اجرای کد از راه دور موجود در Chakra Core به دلیل نحوه نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت چاکرا ایجاد می‌شود. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت.<br>• برنامه ها را نصب و یا حذف کند<br>• می تواند به مشاهده، تغییریا حذف داده ها بپردازد.<br>• حساب کاربری جدید با حقوق کامل برای خود بسازد.<br>•یک در پشتی ایجاد کند. و ...<br>به دلیل اینکه سورس کد موتور چاکرا در گیتاپ مایکروسافت وجود دارد هکرها با بررسی سورس کد برنامه موفق به کشف آسیب پذیری در آن شدند. |

| | |
|---|---|
| رفع آسیب‌پذیری | https://github.com/Microsoft/ChakraCore/wiki/Roadmap#v<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۰۵<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۱۰<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۱۱<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۱۳ |

| | |
|---|---|
| نام محصول | **Chakra Core** |
| نام آسیب‌پذیری | **Scripting Engine Memory Corruption Vulnerability** |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۵۰۰ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | **۲۰۱۸/۱۰/۹** |
| سیستم‌عامل | - |
| توضیحات | آسیب پذیری اجرای کد از راه دور موجود در Chakra Core به دلیل نحوه نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت چاکرا ایجاد می‌شود. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. به دلیل اینکه سورس کد موتور چاکرا در گیتاپ مایکروسافت وجود دارد هکرها با بررسی سورس کد برنامه موفق به کشف آسیب پذیری در آن شدند. |
| رفع آسیب‌پذیری | https://github.com/Microsoft/ChakraCore/wiki/Roadmap#v<br>https://github.com/Microsoft/ChakraCore/releases/tag/v<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۰۰ |

| | |
|---|---|
| نام محصول | Microsoft Edge |
| نام آسیب‌پذیری | Microsoft Edge Memory Corruption Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۴۷۳<br>CVE-۲۰۱۸-۸۵۰۹ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | **۲۰۱۸/۱۰/۹** |
| سیستم‌عامل | Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows Server 2019<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for x64-based Systems |
| توضیحات | آسیب پذیری اجرای کد از راه دور موجود در Microsoft Edge به دلیل نحوه نادرست قراردادن اشیاء در حافظه ایجاد می‌شود. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت.<br>• برنامه ها را نصب و یا حذف کند<br>• می تواند به مشاهده، تغییریا حذف داده ها بپردازد.<br>• حساب کاربری جدید با حقوق کامل برای خود بسازد.<br>•یک در پشتی ایجاد کند. و ...<br>مهاجم می‌تواند یک وب‌سایت مخصوص را طراحی کند تا از این آسیب پذیری Microsoft Edge استفاده کرده و سپس کاربر را مجبور به مشاهده وب سایت می‌کند. مهاجم همچنین می‌تواند از وب‌سایت‌هایی که محتوای نامناسب یا تبلیغاتی دارند استفاده کرده تا کاربران را به این سو هدایت کنند که آن را از طریق اضافه کردن محتوایی ویژه‌ای که می‌تواند از آسیب‌پذیری بهره‌برداری کند، استفاده کنند. |
| رفع آسیب‌پذیری | https://support.microsoft.com/en-us/help/۴۴۶۴۳۳۰/windows-۱۰-update-kb۴۴۶۴۳۳۰<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۴۳۳۰ |

| | |
|---|---|
| | https://support.microsoft.com/en-us/help/۴۴۶۲۹۱۸/windows-۱۰-update-kb۴۴۶۲۹۱۸<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۱۸<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۷۳<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۵۰۹ |

| نام محصول | Microsoft Edge |
|---|---|
| نام آسیب‌پذیری | Chakra Scripting Engine Memory Corruption Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۵۰۵<br>CVE-۲۰۱۸-۸۵۱۰<br>CVE-۲۰۱۸-۸۵۱۱<br>CVE-۲۰۱۸-۸۵۱۳ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | ۲۰۱۸/۱۰/۹ |
| سیستم‌عامل | Windows 10 Version 1803 for x64-based Systems<br>Windows 10 Version 1803 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows Server 2012 R2<br>Windows 10 for 32-bit Systems<br>Windows Server 2016<br>Windows 10 Version 1703 for x64-based Systems<br>Windows 10 Version 1703 for 32-bit Systems<br>Windows 10 Version 1709 for 32-bit Systems<br>Windows 10 Version 1709 for x64-based Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows Server 2016 |

| | |
|---|---|
| | Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems |
| **توضیحات** | آسیب پذیری اجرای کد از راه دور موجود در Microsoft Edge به دلیل نحوه نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت چاکرا ایجاد می‌شود. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت.<br>• برنامه ها را نصب و یا حذف کند<br>• می تواند به مشاهده، تغییریا حذف داده ها بپردازد.<br>• حساب کاربری جدید با حقوق کامل برای خود بسازد.<br>•یک در پشتی ایجاد کند. و ...<br>به دلیل اینکه سورس کد موتور چاکرا در گیتاپ مایکروسافت وجود دارد هکرها با بررسی سورس کد برنامه موفق به کشف آسیب پذیری در آن شدند. |
| **رفع آسیب‌پذیری** | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۶۷<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۶۵<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۶۶<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۶۷<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۵۷۱۳۸<br>https://support.microsoft.com/en-us/help/۴۴۵۷۱۳۸/windows-۱۰-update-kb۴۴۵۷۱۳۸<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۵۷۱۳۱<br>https://support.microsoft.com/en-us/help/۴۴۵۷۱۳۱/windows-۱۰-update-kb۴۴۵۷۱۳۱ |

| | |
|---|---|
| نام محصول | Internet Explorer ۱۱ |
| نام آسیب پذیری | Internet Explorer Memory Corruption Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۴۶۰<br>CVE-۲۰۱۸-۸۴۹۱ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | ۲۰۱۸/۱۰/۹ |
| سیستم‌عامل | Windows Server ۲۰۱۲ R۲<br>Windows Server ۲۰۱۹<br>Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۱<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems<br>Windows ۷ for x۶۴-based Systems Service Pack ۱ |

| | |
|---|---|
| Windows ۱۰ for x۶۴-based Systems<br>Windows ۷ for ۳۲-bit Systems Service Pack ۱<br>Windows Server ۲۰۱۲ R۲<br>Windows ۱۰ for ۳۲-bit Systems<br>Windows RT ۸.۱<br>Windows Server ۲۰۱۶<br>Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۶۴-based Systems | |
| آسیب‌پذیری اجرای کد از راه دور در Internet Explorer ۱۱ زمانی‌که دسترسی نادرست به اشیا در حافظه انجام می‌گیرد وجود دارد. این آسیب‌پذیری می‌تواند حافظه را خراب کرده و به مهاجمین اجازه اجرای کد دلخواه در محتوای کاربر را دهد. | توضیحات |
| https://support.microsoft.com/en-us/help/۴۴۶۲۹۲۶/windows-۸-update-kb۴۴۶۲۹۲۶<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۲۶<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۴۹<br>https://support.microsoft.com/en-us/help/۴۴۶۲۹۴۹/cumulative-security-update-for-internet-explorer<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۶۰<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۹۱ | رفع آسیب‌پذیری |

| | |
|---|---|
| Windows | نام محصول |
| Windows Hyper-V Remote Code Execution Vulnerability | نام آسیب پذیری |
| Critical | حساسیت |
| CVE-۲۰۱۸-۸۴۸۹<br>CVE-۲۰۱۸-۸۴۹۰ | شناسه آسیب‌پذیری |
| Remote Code Execution | تاثیر |

| آخرین به‌روزرسانی | ۲۰۱۸/۱۰/۹ |
|---|---|
| سیستم‌عامل | Windows Server ۲۰۱۲ R۲<br>Windows Server ۲۰۱۹<br>Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۱<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems<br>Windows ۷ for x۶۴-based Systems Service Pack ۱<br>Windows ۱۰ for x۶۴-based Systems<br>Windows ۷ for ۳۲-bit Systems Service Pack ۱<br>Windows Server ۲۰۱۲ R۲<br>Windows ۱۰ for ۳۲-bit Systems<br>Windows RT ۸.۱<br>Windows Server ۲۰۱۶<br>Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۶۴-based Systems |
| توضیحات | آسیب پذیری اجرای کد از راه دور زمانیکه Windows Hyper-V بر روی یک سرور میزبان به صورت صحیحی نمی‌تواند ورودی یک کاربر معتبر بر روی یک سیستم‌عامل مهمان اعتبارسنجی کند وجود دارد. مهاجمی که این آسیب‌پذیری را اکسپلویت کند می‌تواند یک برنامه مخصوص طراحی شده بر روی یک سیستم‌عامل مهمان برای اجرای کد دلخواه را فراهم کند.<br>یک مهاجم که اکسپلویت موفقیت‌آمیز از این آسیب‌پذیری داشته باشد قادر است کد دلخواه را بر روی سیستم‌عامل میزبان اجرا کند. |
| رفع آسیب‌پذیری | https://support.microsoft.com/en-us/help/۴۴۶۲۹۲۳/windows-۷-update-kb۴۴۶۲۹۲۳ |

| | |
|---|---|
| https://support.microsoft.com/en-us/help/۴۴۶۲۹۱۵/windows-۷-update-kb۴۴۶۲۹۱۵<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۲۳<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۱۵<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۸۹<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۹۰ | |

| | |
|---|---|
| نام محصول | Windows |
| نام آسیب‌پذیری | MS XML Remote Code Execution Vulnerability |
| حساسیت | Critical |
| شناسه آسیب‌پذیری | CVE-۲۰۱۸-۸۴۹۴ |
| تاثیر | Remote Code Execution |
| آخرین به‌روزرسانی | ۲۰۱۸/۱۰/۹ |
| سیستم‌عامل | Windows Server ۲۰۱۲ R۲<br>Windows Server ۲۰۱۹<br>Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۱<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for ۳۲-bit systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows ۸.۱ for x۶۴-based systems<br>Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱<br>Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems<br>Windows ۷ for x۶۴-based Systems Service Pack ۱<br>Windows ۱۰ for x۶۴-based Systems<br>Windows ۷ for ۳۲-bit Systems Service Pack ۱<br>Windows Server ۲۰۱۲ R۲<br>Windows ۱۰ for ۳۲-bit Systems<br>Windows RT ۸.۱<br>Windows Server ۲۰۱۶ |

| | |
|---|---|
| | Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems<br>Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems<br>Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۳۲-bit Systems<br>Windows ۱۰ Version ۱۸۰۹ for ۶۴-based Systems |
| توضیحات | آسیب‌پذیری اجرای کد از راه دور زمانیکه Microsoft XML Core Services MSXML ورودی کاربر را پردازش می‌کند وجود دارد. مهاجم می‌تواند با بهره‌برداری موفقیت‌آمیز از این آسیب‌پذیری، کد مخرب را از راه دور اجرا کرده و کنترل سیستم آلوده را به دست بگیرد. |
| رفع آسیب‌پذیری | https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۲۹<br>https://support.microsoft.com/en-us/help/۴۴۶۲۹۲۹/windows-server-۲۰۱۲-update-kb۴۴۶۲۹۲۹<br>https://support.microsoft.com/en-us/help/۴۴۶۲۹۳۱/windows-server-۲۰۱۲-update-kb۴۴۶۲۹۳۱<br>https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۴۶۲۹۳۱<br>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۹۴ |