گزارش اصلاحیه امنیتی مایکروسافت در ماه آگوست 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 آگوست سال ۲۰۱۸ برای محصولات در درجه حساسیت بحرانی[۱] به صورت زیر بوده است:

- Adobe Flash Player
- ChakraCore
- Microsoft Exchange Server
- Microsoft Edge
- Internet Explorer
- Microsoft SQL Server
- Windows

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

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

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ecb۲۶۴۲۵-۵۸۳f-e۸۱۱-a۹۶f-۰۰۰d۳a۳۳c۵۷۳

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	**Adobe Flash Player**
نام آسیب‌پذیری	**Flash Player arbitrary code execution**
حساسیت	**Critical**
شناسه آسیب‌پذیری	**APSB۱۸-۲۵**
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	**۲۰۱۸/۸/۱۴**
سیستم‌عامل	Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1511 for 32-bit Systems Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows Server 2012 Windows 10 for 32-bit Systems Windows Server 2012 R2 Windows 10 for 32-bit Systems Windows RT 8.1 Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems
توضیحات	شناسه‌های آسیب‌پذیری موجود در بیانیه امنیتی Adobe به‌صورت زیر است: CVE-۲۰۱۸-۱۲۸۲۴, CVE-۲۰۱۸-۱۲۸۲۵, CVE-۲۰۱۸-۱۲۸۲۶, CVE-۲۰۱۸-۱۲۸۲۷, CVE-۲۰۱۸-۱۲۸۲۸
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV۱۸۰۰۲۰ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۲/security-update-for-adobe-flash-player

نام محصول	Chakra Core
نام آسیب‌پذیری	Chakra Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۲۶۶ CVE-۲۰۱۸-۸۲۸۰ CVE-۲۰۱۸-۸۲۸۱ CVE-۲۰۱۸-۸۲۸۴
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 for x64-based Systems Windows Server 2012 R2 Windows 10 for 32-bit Systems Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ... 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#v۱۱۰۲ https://github.com/Microsoft/ChakraCore/releases/tag/v۱.۱۰.۲

نام محصول	Chakra Core
نام آسیب‌پذیری	Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۲۵۵ CVE-۲۰۱۸-۸۲۵۹ CVE-۲۰۱۸-۸۲۷۲ CVE-۲۰۱۸-۸۲۸۵ CVE-۲۰۱۸-۸۲۹۰
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows 8.1 for 32-bit systems Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows 8.1 for x64-based systems Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows 10 Version 1511 for 32-bit Systems Windows 10 Version 1511 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 7 for x64-based Systems Service Pack 1 Windows 10 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2012 R2 Windows 10 for 32-bit Systems Windows RT 8.1 Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2

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#v۱۱۰۲ https://github.com/Microsoft/ChakraCore/releases/tag/v۱.۱۰.۲ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۹۰

نام محصول	**Microsoft Exchange Server**
نام آسیب‌پذیری	**Microsoft Exchange Memory Corruption Vulnerability**
حساسیت	**Critical**
شناسه آسیب‌پذیری	**CVE-۲۰۱۸-۸۳۰۲**
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	**۲۰۱۸/۸/۱۴**
سیستم‌عامل	Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 23 Microsoft Exchange Server 2013 Cumulative Update 20 Microsoft Exchange Server 2013 Cumulative Update 21 Microsoft Exchange Server 2016 Cumulative Update 10 Microsoft Exchange Server 2016 Cumulative Update 9
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در نرم‌افزار Microsoft Exchange زمانیکه نرم‌افزار قادر به مدیریت اشیا در حافظه نیست به وجود می‌آید. مهاجم می‌تواند با سواستفاده موفقیت‌آمیز از این آسیب‌پذیری کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند.
رفع آسیب‌پذیری	https://support.microsoft.com/en-us/help/۴۳۴۰۷۳۱/description-of-the-security-update-for-microsoft-exchange-server-۲۰۱۳ https://www.microsoft.com/en-us/download/details.aspx?id=۵۷۲۱۷ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۰۲

نام محصول	**Microsoft Edge**
نام آسیب‌پذیری	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	**Critical**
شناسه آسیب‌پذیری	**CVE-۲۰۱۸-۸۲۵۵** **CVE-۲۰۱۸-۸۲۷۲** **CVE-۲۰۱۸-۸۲۸۵** **CVE-۲۰۱۸-۸۲۹۰**
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	**۲۰۱۸/۸/۱۴**
سیستم‌عامل	Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows Server 2012 Windows 8.1 for 32-bit systems Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows 8.1 for x64-based systems Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows 10 Version 1511 for 32-bit Systems Windows 10 Version 1511 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 7 for x64-based Systems Service Pack 1 Windows 10 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2012 R2 Windows 10 for 32-bit Systems Windows RT 8.1

	Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems
توضیحات	آسیب پذیری اجرای کد از راه دور موجود در مرورگرهای مایکروسافت به دلیل نحوه نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت 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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://support.microsoft.com/en-us/help/۴۳۴۳۸۸۷/windows-۱۰-update-kb۴۳۴۳۸۸۷ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۸۸۷ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۵۵ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۷۲ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۸۵ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۹۰

نام محصول	Microsoft Edge
نام آسیب‌پذیری	Microsoft Edge Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۳۷۷ CVE-۲۰۱۸-۸۳۸۷ CVE-۲۰۱۸-۸۴۰۳
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows Server 2016 Windows Server 2012 Windows Server 2012 R2 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for 32-bit Systems Windows RT 8.1 Windows 10 for x64-based Systems Windows 8.1 for x64-based systems

	Windows 8.1 for 32-bit systems Windows 7 for 32-bit Systems Service Pack 1
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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ... 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۰۳ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۸۷ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۷۷ https://support.microsoft.com/en-us/help/۴۳۴۳۸۹۷/windows-۱۰-update-kb۴۳۴۳۸۹۷ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۹ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۹/windows-۱۰-update-kb۴۳۴۳۹۰۹ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۸۸۵ https://support.microsoft.com/en-us/help/۴۳۴۳۸۸۵/windows-۱۰-update-kb۴۳۴۳۸۸۵

نام محصول	Microsoft Edge
نام آسیب‌پذیری	Chakra Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۲۶۶ CVE-۲۰۱۸-۸۲۸۰ CVE-۲۰۱۸-۸۲۸۱
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 for x64-based Systems Windows Server 2012 R2 Windows 10 for 32-bit Systems Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ... 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-۲۰۱۸-۸۳۸۱ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۸۰ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۲۶۶ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۹ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۹/windows-۱۰-update-kb۴۳۴۳۹۰۹ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۸۸۵ https://support.microsoft.com/en-us/help/۴۳۴۳۸۸۵/windows-۱۰-update-kb۴۳۴۳۸۸۵ https://support.microsoft.com/en-us/help/۴۳۴۳۸۸۷/windows-۱۰-update-kb۴۳۴۳۸۸۷

نام محصول	**Internet Explorer ۱۱**
نام آسیب‌پذیری	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	**Critical**
شناسه آسیب‌پذیری	**CVE-۲۰۱۸-۸۳۵۵** **CVE-۲۰۱۸-۸۳۷۱** **CVE-۲۰۱۸-۸۳۷۲** **CVE-۲۰۱۸-۸۳۷۳** **CVE-۲۰۱۸-۸۳۸۵** **CVE-۲۰۱۸-۸۴۰۳**
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	**۲۰۱۸/۸/۱۴**
سیستم‌عامل	Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۲ Windows Server ۲۰۰۸ for ۳۲-bit Systems Service Pack ۲ Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for x۶۴-based systems

	Windows ۸.۱ for x۶۴-based systems Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems Windows ۷ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ for x۶۴-based Systems Windows ۷ for ۳۲-bit Systems Service Pack ۱ Windows Server ۲۰۱۲ R۲ Windows ۱۰ for ۳۲-bit Systems Windows RT ۸.۱ Windows Server ۲۰۱۶ Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در Internet Explorer ۱۱ به دلیل نحوه نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت 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. مهاجمی که از این آسیب‌پذیری با موفقیت بهره‌برداری کند قادر به داشتن سطح دسترسی همان کاربر خواهد بود که اگر کاربر دارای سطح دسترسی ادمین باشد مهاجم قادر به کنترل سیستم آلوده خواهد بود.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۵۵ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۷۱ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۷۲ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۷۳ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۸۵ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۴۰۳ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۰/windows-۷-update-kb۴۳۴۳۹۰۰ https://support.microsoft.com/en-us/help/۴۳۴۳۲۰۵/cumulative-security-update-for-internet-explorer https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۰ https://support.microsoft.com/en-us/help/۴۳۴۳۸۹۸/windows-۸۱-update-kb۴۳۴۳۸۹۸

نام محصول	Microsoft SQL Server
نام آسیب‌پذیری	Microsoft SQL Server Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۲۷۳
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴

سیستم‌عامل	Microsoft SQL Server 2016 for x64-based Systems Service Pack 1Microsoft Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU) Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU) Microsoft SQL Server 2017 for x64-based Systems Microsoft SQL Server 2017 for x64-based Systems (CU)
توضیحات	آسیب‌پذیری سرریز بافر موجود در Microsoft SQL که اجازه اجرای کد از راه دور بر روی سیستم آلوده را می‌دهد. مهاجم می‌تواند با سواستفاده موفقیت‌آمیز از این آسیب‌پذیری کد دلخواه را در محتوای سرویس اکانت پایگاه داده SQL Server اجرا کند.
رفع آسیب‌پذیری	https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۸/security-update-for-remote-code-execution-vulnerability-in-sql-server https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۱/security-update-for-remote-code-execution-vulnerability-in-sql-server https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۳/description-of-the-security-update-for-the-remote-code-execution-vulne https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۵/security-update-for-remote-code-execution-vulnerability-in-sql-server https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۲/description-of-the-security-update-for-the-remote-code-execution-vulne https://support.microsoft.com/en-us/help/۴۲۹۳۸۰۷/description-of-the-security-update-for-the-remote-code-execution-vulne https://www.microsoft.com/en-us/download/details.aspx?id=۵۷۲۶۷ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۲۷۳

نام محصول	**Windows**
نام آسیب‌پذیری	**GDI+ Remote Code Execution Vulnerability**
حساسیت	**Critical**

شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۳۹۷
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows ۷ for ۳۲-bit Systems Service Pack ۱ Windows ۷ for x۶۴-based Systems Service Pack ۱ Windows Server ۲۰۰۸ for ۳۲-bit Systems Service Pack ۲ Windows Server ۲۰۰۸ for ۳۲-bit Systems Service Pack ۲ (Server Core installation) Windows Server ۲۰۰۸ for Itanium-Based Systems Service Pack ۲ Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۲ Windows Server ۲۰۰۸ for x۶۴-based Systems Service Pack ۲ (Server Core installation) Windows Server ۲۰۰۸ R۲ for Itanium-Based Systems Service Pack ۱ Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱ Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱ (Server Core installation)
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در Windows Graphics Device Interface (GDI) مدیریت اشیا در حافظه بوده است. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم بتواند کنترل سیستم آلوده را به دست بگیرد. مهاجمی که از این آسیب‌پذیری با موفقیت بهره‌برداری کند قادر به داشتن سطح دسترسی همان کاربر خواهد بود که اگر کاربر دارای سطح دسترسی ادمین باشد مهاجم قادر به کنترل سیستم آلوده خواهد بود.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۹۷ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۰ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۸۹۹ https://support.microsoft.com/en-us/help/۴۳۴۳۸۹۹/windows-۷-update-kb۴۳۴۳۸۹۹ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۰/windows-۷-update-kb۴۳۴۳۹۰۰

نام محصول	**Windows**
نام آسیب‌پذیری	**Windows PDF Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	**CVE-۲۰۱۸-۸۳۵۰**
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems Windows Server, version ۱۷۰۹ (Server Core Installation) Windows Server, version ۱۸۰۳ (Server Core Installation)
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در کتابخانه Microsoft Windows PDF که به صورت غیر مستقیم مدیریت اشیا در حافظه را انجام می‌دهد. 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. مهاجمی که از این آسیب‌پذیری با موفقیت بهره‌برداری کند قادر به داشتن سطح دسترسی همان کاربر خواهد بود که اگر کاربر دارای سطح دسترسی ادمین باشد مهاجم قادر به کنترل سیستم آلوده خواهد بود.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۵۰ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۸۸۵ https://support.microsoft.com/en-us/help/۴۳۴۳۸۸۵/windows-۱۰-update-kb۴۳۴۳۸۸۵ https://support.microsoft.com/en-us/help/۴۳۴۳۸۹۷/windows-۱۰-update-kb۴۳۴۳۸۹۷

نام محصول	Windows
نام آسیب‌پذیری	LNK Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۳۴۵
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems Windows Server ۲۰۱۲ Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for x۶۴-based systems Windows ۸.۱ for x۶۴-based systems Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ Version ۱۵۱۱ for ۳۲-bit Systems Windows ۱۰ Version ۱۵۱۱ for x۶۴-based Systems Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems Windows ۷ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ for x۶۴-based Systems Windows ۷ for ۳۲-bit Systems Service Pack ۱ Windows Server ۲۰۱۲ R۲ Windows ۱۰ for ۳۲-bit Systems Windows RT ۸.۱ Windows Server ۲۰۱۶ Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems
توضیحات	آسیب پذیری اجرای کد از راه دور موجود در Microsoft Windows که اگر فایل LNK. پردازش شود اجازه اجرای کد از راه دور را می‌دهد. 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. • برنامه ها را نصب و یا حذف کند

	• می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۴۵ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۰۹۳۹ https://support.microsoft.com/en-us/help/۴۳۴۰۹۳۹/security-update-for-vulnerabilities-in-windows-server-۲۰۰۸ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۰/windows-۷-update-kb۴۳۴۳۹۰۰ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۰ https://support.microsoft.com/en-us/help/۴۳۴۳۸۹۹/windows-۷-update-kb۴۳۴۳۸۹۹

نام محصول	Windows
نام آسیب‌پذیری	Microsoft Graphics Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۸۳۴۴
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	۲۰۱۸/۸/۱۴
سیستم‌عامل	Windows ۱۰ Version ۱۸۰۳ for x۶۴-based Systems Windows ۱۰ Version ۱۸۰۳ for ۳۲-bit Systems Windows Server ۲۰۱۲ Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for ۳۲-bit systems Windows ۸.۱ for x۶۴-based systems Windows ۸.۱ for x۶۴-based systems Windows Server ۲۰۰۸ R۲ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ Version ۱۵۱۱ for ۳۲-bit Systems Windows ۱۰ Version ۱۵۱۱ for x۶۴-based Systems Windows ۱۰ Version ۱۶۰۷ for x۶۴-based Systems Windows ۱۰ Version ۱۶۰۷ for ۳۲-bit Systems Windows ۷ for x۶۴-based Systems Service Pack ۱ Windows ۱۰ for x۶۴-based Systems Windows ۷ for ۳۲-bit Systems Service Pack ۱ Windows Server ۲۰۱۲ R۲ Windows ۱۰ for ۳۲-bit Systems Windows RT ۸.۱ Windows Server ۲۰۱۶ Windows ۱۰ Version ۱۷۰۳ for x۶۴-based Systems

	Windows ۱۰ Version ۱۷۰۳ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۳۲-bit Systems Windows ۱۰ Version ۱۷۰۹ for ۶۴-based Systems
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در کتابخانه Windows font که به صورت غیرمستقیم به خصوص از طریق فونت‌های جاسازی شده خود را نشان می‌دهد. مهاجم می‌تواند با بهره‌برداری موفقیت‌آمیز از این آسیب‌پذیری کنترل سیستم آلوده را به دست بگیرد.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-۲۰۱۸-۸۳۴۴ https://support.microsoft.com/en-us/help/۴۳۴۴۱۰۴/security-update-for-font-library-vulnerability-in-windows https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۴۱۰۴ https://www.catalog.update.microsoft.com/Search.aspx?q=KB۴۳۴۳۹۰۰ https://support.microsoft.com/en-us/help/۴۳۴۳۹۰۰/windows-۷-update-kb۴۳۴۳۹۰۰