گزارش اصلاحیه امنیتی مایکروسافت در ماه 2019 October

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 October سال ۲۰۱۹ برای محصولات در درجه حساسیت بحرانی[1] به صورت زیر بوده است:

- Windows
- Internet Explorer
- Microsoft Edge
- ChakraCore
- Azure App Service

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

نام محصول	Chakra Core Microsoft Edge (Edge HTML - based), Internet Explorer
نام آسیب‌پذیری	Chakra Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1307 CVE-2019-1308 CVE-2019-1335 CVE-2019-1366
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	10/08/2019
سیستم‌عامل	Windows Server 2016 Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows Server 2019 Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for x64-based Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1709 for 32-bit Systems
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 ممووری 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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییر یا 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-2019-1307 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1308 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1335 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1366

نام محصول	**Azure App Service on Azure Stack**
نام آسیب‌پذیری	**Azure App Service Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1372
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	10/08/2019
محصولات آسیب پذیر	Azure App Service on Azure Stack
توضیحات	آسیب‌پذیری اجرای کد از راه دور در Azure App Service/ Antares بر روی Azure Stack وجود دارد که نمیتواند قبل از کپی کردن طول بافر را اندازه بگیرد. مهاجمی که با موفقیت از این آسیب‌پذیری بهره برداری کرده است می تواند یک عملکرد unprivileged توسط کاربر مجاز را اجرا کند تا بتواند کد را در متن NT AUTHORITY\system را اجرا کند و بدین ترتیب از محیط sandbox فرارکند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1372

نام محصول	MS XML
نام آسیب‌پذیری	MS XML Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1060
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	10/08/2019
محصولات آسیب پذیر	Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 Version 1903 for x64-based Systems Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server, version 1803 (Server Core Installation) Windows Server, version 1903 (Server Core installation)
توضیحات	آسیب‌پذیری اجرای کد از راه دور زمانی که تحلیل کننده پردازنده Microsoft XML Core Services MSXML ورودی کاربر را پردازش می کند مهاجمی که با موفقیت از آسیب‌پذیری بهره برداری کرده است می‌تواند از راه دور کد مخرب را برای کنترل سیستم کاربر اجرا کند.

رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1060

نام محصول	**windows**
نام آسیب‌پذیری	**Remote Desktop Client Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1333
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	10/08/2019
محصولات آسیب پذیر	Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 Version 1903 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for Itanium-Based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

	Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server, version 1803 (Server Core Installation) Windows Server, version 1903 (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. • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییر یا 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-2019-1333

نام محصول	Internet Explorer
نام آسیب‌پذیری	VBScript Engine Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1238
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	10/08/2019
سیستم‌عامل	Windows Server 2012 Windows 10 Version 1703 for 32-bit Systems Windows 10 Version 1703 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows Server 2019 Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for x64-based Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows Server 2016 Windows 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2
توضیحات	یک آسیب‌پذیری اجرای کد از راه دور موجود در موتور VBScript وجود دارد که از اشیاء موجود در حافظه استفاده می‌کند. مهاجم می‌تواند 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 به‌دست آورد و سیستم آسیب دیده را کنترل کند. در نتیجه اگر کاربر با

	حساب کاربری مدیر وارد شود. با این توضیحات، مهاجم توانایی فعالیت‌های زیر را خواهد داشت. • برنامه ها را نصب و یا حذف کند. • می تواند به مشاهده، تغییر یا 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-2019-1238

نام محصول	Internet Explorer
نام آسیب‌پذیری	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1367
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**10/08/2019**
سیستم‌عامل	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows 10 Version 1903 for x64-based Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1703 for x64-based Systems

	Windows 10 Version 1703 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 Windows 10 for 32-bit Systems
توضیحات	یک آسیب‌پذیری اجرایی کد از راه دور موجود در حافظه موتورهای اسکریپتی مرورگر های مایکروسافت وجود دارد این آسیب‌پذیری میتواند حافظه را به گونه ای تخریب کند که مهاجم بتواند کد دلخواه را در زمینه کاربر فعلی اجرا کند یک مهاجم که از این آسیب‌پذیری استفاده کرده است می تواند همان سطح دسترسی کاربر فعلی را بدست آورد .و میتواند سیستم مورد نظر را کنترل 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، تغییر یا 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-2019-1367