گزارش اصلاحیه امنیتی مایکروسافت در ماه سپتامبر ۲۰۱۹

مایکروسافت آخرین به‌روزرسانی را برای آسیب‌پذیری‌های نرم‌افزارها و سیستم‌عامل‌های این شرکت منتشر کرده است. به‌روزرسانی امنیتی در ماه سپتامبر سال ۲۰۱۹ برای محصولات در درجه حساسیت بحرانی[1] به صورت زیر بوده است:

- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- ChakraCore
- Microsoft SharePoint
- Azure DevOps Server

و همچنین برای Adobe Flash Player یک بروزرسانی با شناسه ADV190022 ارائه شد.

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	**Adobe Flash Player**
بروزرسانی	**September 2019 Adobe Flash Security Update**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-8069 CVE-2019-8070
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
سیستم‌عامل	Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows Server 2012 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based 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 1709 for 64-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 x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows Server 2019 Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1903 for ARM64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for x64-based Systems
توضیحات	این به‌روزرسانی امنیتی مربوط به آسیب پذیری با شناسه CVE-2019-8069 و CVE-2019-8070 می‌باشد. سواستفاده موفق از این آسیب‌پذیری منجر به اجرای کد از راه دور می‌شود.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190022

نام محصول	**Chakra Core** **Microsoft Edge (EdgeHTML-based)**
نام آسیب‌پذیری	**Chakra Scripting Engine Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1138 CVE-2019-1217 CVE-2019-1237 CVE-2019-1298 CVE-2019-1300 CVE-2019-1221
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
سیستم‌عامل	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
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. • 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-2019-1300

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1298 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1237 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1217 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1138 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1221	

Azure DevOps Server	نام محصول
Azure DevOps and Team Foundation Server Remote Code Execution Vulnerability	نام آسیب‌پذیری
Critical	حساسیت
CVE-2019-1306	شناسه آسیب‌پذیری
Remote Code Execution	تاثیر
09/10/2019	آخرین به‌روزرسانی
Team Foundation Server 2018 Update 3.2 Azure DevOps Server 2019.0.1 Azure DevOps Server 2019 Update 1	سیستم‌عامل
آسیب‌پذیری اجرای کد از راه دور موجود در Azure DevOps Server (ADO) و Team Foundation Server (TFS) که نتواند صحت ورودی را تایید کند، مهاجم که بتواند از این آسیب پذیری استفاده کند توانایی دارد کد مربوط به حساب کاربری TFS یا ADO را روی سرور اجرا کند.	توضیحات
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1306	رفع آسیب‌پذیری

نام محصول	**Internet Explorer**
نام آسیب‌پذیری	**VBScript Engine Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1208 CVE-2019-1236
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
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-2019-1208 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1236

نام محصول	**Microsoft SharePoint**
نام آسیب‌پذیری	**Microsoft SharePoint Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1257 CVE-2019-1295 CVE-2019-1296
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
سیستم‌عامل	Microsoft SharePoint Server 2019 Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Foundation 2010 Service Pack 2 Microsoft SharePoint Enterprise Server 2016
توضیحات	آسیب‌پذیری اجرای کد از راه دور در Microsoft SharePoint وجود دارد که نرم افزار نتواند نشانه‌گذاری منبع بسته نرم‌افزاری را بررسی کند. مهاجمی که با موفقیت از این آسیب‌پذیری سوء استفاده کند، قادر است کد دلخواه را در زمینه SharePoint application pool و SharePoint server farm account اجرا کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1257 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1295 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1296

نام محصول	**Windows**
نام آسیب‌پذیری	**Remote Desktop Client Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1290 CVE-2019-1291 CVE-2019-0788 CVE-2019-0787
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
سیستم‌عامل	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-2019-1290 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1291 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0788 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0787

نام محصول	**Windows**
نام آسیب‌پذیری	**LNK Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1280
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	09/10/2019
سیستم‌عامل	Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for Itanium-Based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows RT 8.1 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 در ویندوز مایکروسافت وجود دارد که در صورت پردازش یک فایل LNK.، امکان اجرای کد از راه دور وجود دارد. مهاجم که از این آسیب‌پذیری استفاده کرده باشد، می‌تواند دسترسی کاربر محلی را به‌دست آورد.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1280