گزارش اصلاحیه امنیتی مایکروسافت در ماه مارس ۲۰۲۰

مایکروسافت آخرین به‌روزرسانی را برای آسیب‌پذیری‌های نرم‌افزارها 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 مارس سال ۲۰۲۰** شامل موارد زیر برای محصولات مایکروسافت در درجه حساسیت بحرانی[1] بوده است.

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- ChakraCore
- Internet Explorer
- Microsoft Office and Microsoft Office Services and Web Apps
  - Microsoft Guidance for Disabling SMBv3 Compression

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	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0768 CVE-2020-0823 CVE-2020-0848 CVE-2020-0811 CVE-2020-0812 CVE-2020-0825 CVE-2020-0826 CVE-2020-0827 CVE-2020-0828 CVE-2020-0829 CVE-2020-0830 CVE-2020-0831 CVE-2020-0832 CVE-2020-0833 CVE-2020-0816
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/10/2020
سیستم‌عامل	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 1909 for 32-bit Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for x64-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 اسکریپت محصولات ذکر شده 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-2020-0816 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0833 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0831 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0829 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0828 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0827 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0826 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0825 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0812 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0811 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0848 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0823 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0768

نام محصول	Internet Explorer
نام آسیب‌پذیری	VBScript Engine Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0847
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	03/10/2020
سیستم‌عامل	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 1909 for 32-bit Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for x64-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-2020-0847

نام محصول	Microsoft Office
نام آسیب‌پذیری	**Microsoft Word Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0852
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/10/2020
سیستم‌عامل	Microsoft Office 2016 for Mac Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office Online Server Microsoft SharePoint Server 2019
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. برای استفاده از این آسیب‌پذیری کاربر باید فایل word را که توسط مهاجم ساخته شده است با محصولات آسیب‌پذیر اجرا کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0852

نام محصول	Windows
نام آسیب‌پذیری	LNK Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0684
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/10/2020
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 1709 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1709 for x64-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 10 Version 1909 for 32-bit Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 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 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) Windows Server, version 1909 (Server Core installation)
توضیحات	یک آسیب‌پذیری در سیستم‌عامل ویندوز وجود دارد که در صورت پردازش یک فایل LNK.، امکان اجرای کد از راه دور ایجاد می‌شود. مهاجمی 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-2020-0684

نام محصول	**windows**
نام آسیب‌پذیری	**Media Foundation Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0809 CVE-2020-0801 CVE-2020-0807 CVE-2020-0869
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/10/2020
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 1709 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1709 for x64-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 10 Version 1909 for 32-bit Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for x64-based Systems 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) Windows Server, version 1909 (Server Core installation)
توضیحات	آسیب‌پذیری اجرای کد از راه دور در هنگامی که Windows Media Foundation به طور نامناسب فایل‌های QuickTime media دستکاری شده را تجزیه و تحلیل کند، وجود خواهد داشت. مهاجمی که با موفقیت از این آسیب‌پذیری سوءاستفاده کرده است می‌تواند سطح دسترسی کاربر محلی را داشته باشد.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0869 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0807 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0801 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0809

نام محصول	**windows**
نام آسیب‌پذیری	**GDI+ Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-0883 CVE-2020-0881
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/10/2020

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 1709 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1709 for x64-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 10 Version 1909 for 32-bit Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 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) Windows Server, version 1909 (Server Core installation)

توضیحات	این آسیب‌پذیری اجرا کد از راه‌دور در واسط دستگاه گرافیکی ویندوز (GDI) به واسطه کنترل نامناسب اشیاء موجود در حافظه ایجاد می‌شود. 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-2020-0883 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0881

نام محصول	**Security Advisory**
نام	**Microsoft Guidance for Disabling SMBv3 Compression**
شناسه	ADV200005
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	03/11/2020
سیستم‌عامل	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 10 Version 1909 for 32-bit Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for x64-based Systems Windows Server, version 1909 (Server Core installation) Windows Server, version 1903 (Server Core installation)
توضیحات	مایکروسافت آگاهی‌رسانی را درخصوص آسیب‌پذیری بر روی SMBv3 که امکان اجرای کد از راه دور و توزیع کرم‌گونه را بر روی سیستم‌های آسیب‌پذیر فراهم می‌نماید را انجام داده است. مهاجم که با موفقیت از آسیب‌پذیری سوءاستفاده کرده‌است می‌تواند قابلیت اجرا کد را در سرور SMB هدف یا SMB Client به دست آورد. توصیه می‌شود قابلیت فشرده‌سازی SMBv3 را غیرفعال کرده و پورت ۴۴۵ رو هم ببندید.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200005