گزارش اصلاحیه امنیتی مایکروسافت در ماه 2019 July

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

- ChakraCore
- Microsoft Edge
- Internet Explorer
- Windows

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	**windows**
نام آسیب‌پذیری	**Windows DHCP Server Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-0785
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
سیستم‌عامل	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 مخرب حافظه در سرویس DHCP ویندوز سرور وجود دارد. مهاجم قادر است که بسته‌های ویژه‌ای را به یک سرور DHCP بفرستد و می‌تواند با استفاده از این آسیب‌پذیری کدهای دلخواه خود را در سرور DHCP اجرا کند و یا آن را از دسترس خارج کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0785

نام محصولات	**Internet Explorer 11** **Microsoft Edge**
نام آسیب‌پذیری	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1001 CVE-2019-1004 CVE-2019-1056 CVE-2019-1059
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
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 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 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 حافظه موتورهای اسکریپتی مرورگرهای مایکروسافت وجود دارد. این آسیب‌پذیری می‌تواند حافظه را به گونه‌ای تخریب کند که مهاجم را قادر سازد که کد دلخواه را در زمینه کاربر فعلی اجرا کند. یک مهاجم که از این آسیب‌پذیری استفاده کرده است می‌تواند همان سطح دسترسی کاربر فعلی را بدست آورد و سیستم مورد نظر را کنترل کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت‌های زیر را خواهد داشت: • برنامه‌ها را نصب و یا حذف کند. • می‌تواند به مشاهده، تغییر یا حذف داده‌ها 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-2019-1001

نام محصول	Chakra Core
نام آسیب‌پذیری	Chakra Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1062 CVE-2019-1092 CVE-2019-1103 CVE-2019-1106 CVE-2019-1107
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
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. آسیب‌پذیری می تواند 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، می تواند 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-2019-1062

نام محصول	Team Foundation Server-Azure DevOps Server
نام آسیب‌پذیری	Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1072
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
سیستم‌عامل	Azure DevOps Server 2019.0.1 Team Foundation Server 2010 SP1 (x64) Team Foundation Server 2010 SP1 (x86) Team Foundation Server 2012 Update 4 Team Foundation Server 2013 Update 5 Team Foundation Server 2015 Update 4.2 Team Foundation Server 2017 Update 3.1 Team Foundation Server 2018 Update 1.2 Team Foundation Server 2018 Update 1.2
توضیحات	زمانی که Azure DevOps Server و Team Foundation Server (TFS) به شکل نادرست از ورودی کاربر استفاده می‌کنند، یک آسیب‌پذیری اجرایی کد از راه دور وجود دارد. مهاجمی که آسیب‌پذیری را با موفقیت مورد سوء استفاده قرار دهد، می‌تواند کد را بر روی سرور مقصد در سرویس Devops یا حساب سرویس TFS اجرا کند و مهاجم دیگر به احراز هویت نیاز ندارد.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1072

نام محصول	Microsoft .NET Framework
نام آسیب‌پذیری	.NET Framework Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1113
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
سیستم‌عامل	Microsoft .NET Framework 3.0 Service Pack 2 Microsoft .NET Framework 3.5 Microsoft .NET Framework 3.5 AND 4.7.2 Microsoft .NET Framework 3.5.1 Microsoft .NET Framework 4.5.2 Microsoft .NET Framework 4.6 Microsoft .NET Framework 4.6/4.6.1/4.6.2 Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 Microsoft .NET Framework 4.8 Microsoft Visual Studio 2017 Microsoft Visual Studio 2017 version 15.9 Microsoft Visual Studio 2019 version 16.0 Microsoft Visual Studio 2019 version 16.1
توضیحات	وقتی که نرم‌افزار نتواند نشانه‌گذاری منبع یک فایل را بررسی کند، یک آسیب‌پذیری اجرای کد از راه دور در فریمورک .NET. وجود دارد. مهاجمی که آسیب پذیری را به خوبی مورد سو، استفاده قرار داده است، می تواند کد دلخواه را در سطح دسترسی کاربر فعلی اجرا کند. اگر کاربر فعلی با سطح دسترسی کاربر وارد سیستم شود مهاجم می تواند کنترل سیستم آسیب دیده را در دست بگیرد و 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-2019-1113

نام محصول	**Microsoft Edge**
نام آسیب‌پذیری	**Internet Explorer Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1063
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
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	زمانی که Internet Explorer به صورت نادرست به اشیاء حافظه دسترسی پیدا کند این مشکل امنیتی ایجاد می‌شود. دستکاری با یک ورودی ناشناخته منجر به آسیب‌پذیری حافظه می شود. مهاجمان می‌توانند از این مسئله برای اجرای کد دلخواه در حساب کاربری مربوط به کاربر جاری، استفاده کنند. در صورتی که یک مهاجم بتواند از این آسیب‌پذیری بهره برداری نماید، می‌تواند حقوق کاربر را به عنوان کاربر فعلی بدست آورد.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1063

نام محصول	**Microsoft Edge**
نام آسیب‌پذیری	**Microsoft Browser Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1104
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
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 System 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 32-bit 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 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 System 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 10 Version 1607 for x64-based Systems
توضیحات	آسیب‌پذیری اجرای کد از راه دور موجود در مرورگرهای مایکروسافت است که به دلیل دسترسی نادرست مرورگرها به اشیا، در داخل حافظه به وجود می‌آید. در صورتی که مهاجم با موفقیت آسیب‌پذیری را مورد سوءاستفاده قرار می‌دهد، می‌تواند همان دسترسی‌های کاربر را به عنوان کاربر فعلی بدست آورد. اگر کاربر فعلی با دسترسی کاربر وارد سیستم شود، مهاجم می تواند کنترل سیستم آسیب دیده را در دست بگیرد. 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-2019-1104

نام محصول	**windows**
نام آسیب‌پذیری	**GDI+ Remote Code Execution Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2019-1102
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	**2019/07/09**
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 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	این آسیب‌پذیری اجرای کد از راه دور است که در هنگامی که رابط گرافیکی ویندوز به مدیریت اشیاء در حافظه می‌پردازد به وجود می‌آید. یک مهاجم که با موفقیت آسیب‌پذیری را مورد سوءاستفاده قرار دهد، می‌تواند همان دسترسی‌های کاربر را به عنوان کاربر فعلی بدست آورد. اگر کاربر فعلی با دسترسی کاربر وارد سیستم شود، مهاجم می‌تواند کنترل سیستم آسیب دیده را بر عهده گیرد. 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 ... در یک سناریو حمله به اشتراک گذاری فایل، مهاجم می‌تواند یک فایل سند مخصوص ساخته شده ایجاد کند که برای سوء استفاده از آسیب‌پذیری طراحی شده و سپس کاربران را متقاعد کند تا فایل سند را باز کنند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1102