بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

اصلاحیه امنیتی مایکروسافت در ماه ژوئن۲۰۲۰

به‌روزرسانی

فهرست مطالب

۱ مقدمه

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 ژوئن سال۲۰۲۰** شامل موارد زیر برای محصولات مایکروسافت در درجه حساسیت **بحرانی(Critical)** بوده است.

- Microsoft Windows
- Microsoft Edge
- Internet Explorer
- Microsoft Office

وصله امنیتی هر کدام از آسیب‌پذیری‌ها بر اساس نسخه خاصی از سیستم‌عامل در گزارش آماده 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.

۲ آسیب‌پذیری‌های بحرانی(Critical)

نام محصول	Chakra Core Microsoft Edge, Internet Explorer
نام آسیب‌پذیری	Scripting Engine Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1219 CVE-2020-1073
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
سیستم‌عامل	Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit 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 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 10 Version 2004 for 32-bit Systems	
Windows 10 Version 2004 for x64-based Systems	
Windows 10 Version 2004 for ARM64-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 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	

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 و 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-2020-1073 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219

نام محصول	Internet Explorer
نام آسیب‌پذیری	VBScript Engine Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1216 CVE-2020-1213 CVE-2020-1260
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
سیستم‌عامل	Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-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 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 10 Version 2004 for 32-bit Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2	
یک آسیب‌پذیری اجرای کد از راه دور در موتور VBScript وجود دارد که از اشیاء موجود در حافظه سوءاستفاده می‌کند و مهاجم را قادر می‌سازد 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 و یا حذف داده‌ها بپردازد. • حساب کاربری جدید با حقوق کامل برای خود بسازد. • یک در پشتی ایجاد کند و ...	توضیحات
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1073 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219	رفع آسیب‌پذیری

نام محصول	Microsoft office
نام آسیب‌پذیری	Microsoft SharePoint Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1181
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	**06/09/2020**
محصولات	Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Foundation 2010 Service Pack 2 Microsoft SharePoint Foundation 2013 Service Pack 1
توضیحات	یک آسیب‌پذیری اجرای کد از راه دور موجود در Microsoft SharePoint محصولات ذکر شده در هنگامی که برنامه قابلیت بررسی نشانگرهای بسته‌ها را نتواند انجام دهد، وجود خواهد داشت. به سبب وجود این آسیب‌پذیری مهاجم خواهد توانست کد دلخواه را در زمینه کاربر فعلی اجرا کند. همچنین یک مهاجم که با موفقیت آسیب‌پذیری را مورد سوءاستفاده قرار دهد، قادر است حساب farm account را اجرا کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1181

نام محصول	Windows
نام آسیب‌پذیری	LNK Remote Code Execution Vulnerability
حساسیت	**Critical**
شناسه آسیب‌پذیری	CVE-2020-1299
تاثیر	**Remote Code Execution**
آخرین به‌روزرسانی	06/09/2020

Windows 10 for 32-bit Systems	سیستم‌عامل
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 10 Version 2004 for 32-bit Systems	
Windows 10 Version 2004 for ARM64-based Systems	
Windows 10 Version 2004 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) Windows Server, version 2004 (Server Core installation)	
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 سوءاستفاده کرده باشد، می‌تواند دسترسی کاربر محلی را به‌دست آورد.	**توضیحات**
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299	**رفع آسیب‌پذیری**

نام محصول	Windows
نام آسیب‌پذیری	Windows Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1300
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
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 10 Version 2004 for 32-bit Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 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) Windows Server, version 2004 (Server Core installation)	
آسیب‌پذیری اجرای کد از راه دور در ویندوز هنگامی که سیستم‌عامل نتواند فایل‌های cabinet را به درستی کنترل و بررسی کند، وجود دارد. برای سوءاستفاده از این آسیب‌پذیری کاربر باید فایل ساخته شده توسط مهاجم را اجرا کند.	**توضیحات**
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1300	**رفع آسیب‌پذیری**

نام محصول	Windows
نام آسیب‌پذیری	Windows OLE Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1281
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
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 10 Version 2004 for 32-bit Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 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) Windows Server, version 2004 (Server Core installation)	
آسیب‌پذیری اجرای کد از راه دور موجود در این محصولات زمانی به‌وجود می‌آید که Microsoft Windows OLE نتواند به درستی اعتبار ورودی کاربر را تأیید کند. یک مهاجم می‌تواند از با سوءاستفاده از این آسیب‌پذیری، اجرای کد مخرب را در سیستم داشته باشد.	**توضیحات**
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1281	**رفع آسیب‌پذیری**

نام محصول	windows
نام آسیب‌پذیری	GDI+ Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1248
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
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 10 Version 2004 for 32-bit Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for x64-based Systems Windows Server, version 1903 (Server Core installation) Windows Server, version 1909 (Server Core installation) Windows Server, version 2004 (Server Core installation)
توضیحات	این آسیب‌پذیری اجرا کد از راه دور 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-2020-1248

نام محصول	Window
نام آسیب‌پذیری	Windows Shell Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2020-1286
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	06/09/2020
سیستم‌عامل	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 10 Version 2004 for 32-bit Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for x64-based Systems 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)

	Windows Server, version 2004 (Server Core installation)
توضیحات	این آسیب‌پذیری اجرای کد از راه دور هنگامی به وجود می‌آید که ویندوز Shell مسیرهای پرونده را به درستی تأیید نکند. 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-2020-1286

نام محصول	**Adobe Flash player**
نام آسیب‌پذیری	**June 2020 Adobe Flash Security Update**
حساسیت	**Critical**
شناسه آسیب‌پذیری	ADV200010
تاثیر	**Update**
آخرین به‌روزرسانی	06/09/2020
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 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2012 Windows Server 2012 R2 Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems	
در این به‌روزرسانی امنیتی به آسیب‌پذیری با شناسه CVE-2020-9633 اشاره دارد، که در بولتن Adobe Security APSB20-30 شرح داده شده است.	**توضیحات**
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200010	**رفع آسیب‌پذیری**

۳ منبع

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