بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه‌ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

آسیب‌پذیری‌های اجرای کد از راه دور در کتابخانه Codecs ویندوز

گزارش آسیب پذیری

شناسه سند	Maher_13990415-1
نوع سند	گزارش فنی
شماره نگارش	۱/۰
تاریخ نگارش	۱۳۹۹/۰۴/۱۳
طبقه‌بندی سند	عادی

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰ (۰۲۱)۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ آسیب‌پذیری‌های اجرای کد از راه دور در کتابخانه Codecs ویندوز

شرکت مایکروسافت به‌روزرسانی امنیتی را جهت وصله دو آسیب‌پذیری موجود در کتابخانه codecs ویندوز منتشر کرد. آسیب‌پذیری‌های مذکور با شناسه CVE-2020-1425 و CVE-2020-1457 بر کتابخانه codecs ویندوز در توزیع‌های ویندوز ۱۰ و ویندوز سرور ۲۰۱۹ اثر می‌گذارند. شرکت مایکروسافت همچنین اظهار داشت که از این دو نقض امنیتی می‌توان توسط یک فایل تصویری دست‌کاری شده خاص بهره‌برداری کرد. اگر این تصاویر در برنامه‌هایی باز شود که از کتابخانه codecs ویندوز، برای مدیریت محتوای چندرسانه‌ای استفاده می‌کند، مهاجم می‌تواند کد مخرب خود را روی سیستم ویندوز اجرا کرده و کنترل کاملی بر آن به دست آورد.

۱-۱ آسیب‌پذیری CVE-2020-1425

این آسیب‌پذیری اجرای کد از راه دور بحرانی در کتابخانه Codecs ویندوز وجود داشته و اشیاء موجود در حافظه را تحت تأثیر قرار می‌دهد. مهاجم با بهره‌برداری از آن می‌تواند اطلاعاتی را به منظور به خطر انداختن سیستم قربانی به دست آورد. بهره‌برداری از این آسیب‌پذیری نیازمند برنامه‌ای جهت پردازش یک فایل تصویری دست‌کاری‌شده‌ی خاص است. با اعمال به‌روزرسانی منتشر شده، پس از تصحیح نحوه مدیریت اشیاء موجود در حافظه توسط کتابخانه codecs ویندوز، این آسیب‌پذیری وصله خواهد شد.

۱-۱-۱ سیستم‌های تحت تأثیر این آسیب‌پذیری

سیستم‌های تحت تاثیر آسیب پذیری CVE-2020-1425 در جدول ۱ نمایش داده شده‌اند.

جدول ۱: سیستم‌های تحت تأثیر آسیب‌پذیری CVE-2020-1425

ردیف	نام محصول	تأثیر	شدت
۱	Windows 10 Version 1709 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۲	Windows 10 Version 1709 for x64-based Systems	اجرای کد از راه دور	بحرانی
۳	Windows 10 Version 1803 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۴	Windows 10 Version 1803 for ARM64-based Systems	اجرای کد از راه دور	بحرانی
۵	Windows 10 Version 1803 for x64-based Systems	اجرای کد از راه دور	بحرانی
۶	Windows 10 Version 1809 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۷	Windows 10 Version 1809 for ARM64-based Systems	اجرای کد از راه دور	بحرانی
۸	Windows 10 Version 1809 for x64-based Systems	اجرای کد از راه دور	بحرانی
۹	Windows 10 Version 1903 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۱۰	Windows 10 Version 1903 for ARM64-based Systems	اجرای کد از راه دور	بحرانی
۱۱	Windows 10 Version 1903 for x64-based Systems	اجرای کد از راه دور	بحرانی

ردیف	نام محصول	تأثیر	شدت
۱۲	Windows 10 Version 1909 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۱۳	Windows 10 Version 1909 for ARM64-based Systems	اجرای کد از راه دور	بحرانی
۱۴	Windows 10 Version 1909 for x64-based Systems	اجرای کد از راه دور	بحرانی
۱۵	Windows 10 Version 2004 for 32-bit Systems	اجرای کد از راه دور	بحرانی
۱۶	Windows 10 Version 2004 for ARM64-based Systems	اجرای کد از راه دور	بحرانی
۱۷	Windows 10 Version 2004 for x64-based Systems	اجرای کد از راه دور	بحرانی
۱۸	Windows Server 2019	اجرای کد از راه دور	بحرانی
۱۹	Windows Server 2019 (Server Core installation)	اجرای کد از راه دور	بحرانی
۲۰	Windows Server, version 1803 (Server Core Installation)	اجرای کد از راه دور	بحرانی
۲۱	Windows Server, version 1903 (Server Core installation)	اجرای کد از راه دور	بحرانی
۲۲	Windows Server, version 1909 (Server Core installation)	اجرای کد از راه دور	بحرانی
۲۳	Windows Server, version 2004 (Server Core installation)	اجرای کد از راه دور	بحرانی
۲۴	Windows 10 Version 1709 for ARM64-based Systems	اجرای کد از راه دور	بحرانی

۲-۱ آسیب‌پذیری CVE-2020-1457

این آسیب‌پذیری اجرای کد از راه دور با شدت بالا در کتابخانه Codecs ویندوز وجود داشته و اشیاء موجود در حافظه را تحت تأثیر قرار می‌دهد. مهاجم با بهره‌برداری از آن می‌تواند با ایجاد یک فایل تصویری دست‌کاری شده خاص و فریب قربانی جهت باز نمودن آن، کد دلخواه خود را روی سیستم قربانی اجرا کرده و منجر به به خطر انداختن کل سیستم شود. بهره‌برداری از این آسیب‌پذیری نیازمند برنامه‌ای به منظور پردازش یک فایل تصویری دست‌کاری شده خاص است. با اعمال به‌روزرسانی منتشر شده، پس از تصحیح نحوه مدیریت اشیاء موجود در حافظه توسط کتابخانه codecs ویندوز، این آسیب‌پذیری وصله خواهد شد.

۱-۲-۱ سیستم‌های تحت تأثیر این آسیب‌پذیری

سیستم‌های تحت تأثیر آسیب‌پذیری CVE-2020-1457 در **Error! Reference source not found.** نمایش داده شده‌اند.

جدول ۲: سیستم‌های تحت تأثیر آسیب‌پذیری CVE-2020-1457

ردیف	نام محصول	تأثیر	شدت
۱	Windows 10 Version 1709 for 32-bit Systems	اجرای کد از راه دور	بالا
۲	Windows 10 Version 1709 for x64-based Systems	اجرای کد از راه دور	بالا
۳	Windows 10 Version 1803 for 32-bit Systems	اجرای کد از راه دور	بالا
۴	Windows 10 Version 1803 for ARM64-based Systems	اجرای کد از راه دور	بالا
۵	Windows 10 Version 1803 for x64-based Systems	اجرای کد از راه دور	بالا

ردیف	نام محصول	تأثیر	شدت
۶	Windows 10 Version 1809 for 32-bit Systems	اجرای کد از راه دور	بالا
۷	Windows 10 Version 1809 for ARM64-based Systems	اجرای کد از راه دور	بالا
۸	Windows 10 Version 1809 for x64-based Systems	اجرای کد از راه دور	بالا
۹	Windows 10 Version 1903 for 32-bit Systems	اجرای کد از راه دور	بالا
۱۰	Windows 10 Version 1903 for ARM64-based Systems	اجرای کد از راه دور	بالا
۱۱	Windows 10 Version 1903 for x64-based Systems	اجرای کد از راه دور	بالا
۱۲	Windows 10 Version 1909 for 32-bit Systems	اجرای کد از راه دور	بالا
۱۳	Windows 10 Version 1909 for ARM64-based Systems	اجرای کد از راه دور	بالا
۱۴	Windows 10 Version 1909 for x64-based Systems	اجرای کد از راه دور	بالا
۱۵	Windows 10 Version 2004 for 32-bit Systems	اجرای کد از راه دور	بالا
۱۶	Windows 10 Version 2004 for ARM64-based Systems	اجرای کد از راه دور	بالا
۱۷	Windows 10 Version 2004 for x64-based Systems	اجرای کد از راه دور	بالا
۱۸	Windows Server 2019	اجرای کد از راه دور	بالا
۱۹	Windows Server 2019 (Server Core installation)	اجرای کد از راه دور	بالا
۲۰	Windows Server, version 1803 (Server Core Installation)	اجرای کد از راه دور	بالا
۲۱	Windows Server, version 1903 (Server Core installation)	اجرای کد از راه دور	بالا
۲۲	Windows Server, version 1909 (Server Core installation)	اجرای کد از راه دور	بالا
۲۳	Windows Server, version 2004 (Server Core installation)	اجرای کد از راه دور	بالا
۲۴	Windows 10 Version 1709 for ARM64-based Systems	اجرای کد از راه دور	بالا

مایکروسافت جزئیات زیادی در مورد این آسیب‌پذیری‌ها منتشر نکرده است، اما حملات با استفاده از روش‌های مشابهی (معمولاً از طریق فریب کاربر جهت بازگشایی یک فایل مخرب) انجام می‌گیرد. به منظور وصله این دو آسیب‌پذیری اجرای کد از راه دور، به‌روزرسانی‌هایی در کتابخانه codecs ویندوز در سیستم‌های کاربران و از طریق برنامه app store ویندوز منتشر گردیده است. جهت دریافت این به‌روزرسانی اقدام خاصی لازم نیست، زیرا این کتابخانه به طور خودکار از طریق برنامه مذکور به‌روزرسانی می‌شود. این آسیب‌پذیری‌ها به طور محرمانه گزارش شده و تا پیش از انتشار این وصله‌ها مورد بهره‌برداری قرار نگرفته بودند.

۲ مراجع

[1] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1425

[2] https://windowsreport.com/microsoft-security-updates-fix-codecs/

[3] https://www.cybersecurity-help.cz/vdb/SB2020063027

[4] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1457

[5] https://www.securityweek.com/windows-codecs-library-vulnerabilities-allow-remote-code-execution

[6] https://www.zdnet.com/article/microsoft-releases-emergency-security-update-to-fix-two-bugs-in-windows-codecs/#ftag=RSSbaffb68