بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

نقص بحرانی در سیستم‌عامل IOS روترهای سیسکو که به هکرهای از راه دور اجازه می‌دهد کنترل کاملی بر سیستم‌ها داشته باشند.

گزارش آسیب‌پذیری

فهرست مطالب

۱ مقدمه

اخیراً سیسکو اعلام کرده‌است که تعداد زیادی آسیب‌پذیری را در سیستم‌عامل IOS روترهایش برطرف کرده‌است که شامل بیش از ده‌ها آسیب‌پذیری است که بر سوئیچ‌ها و روترهای صنعتی شرکت تاثیر می‌گذارند. درمجموع، ۲۵ آسیب‌پذیری با شدت بالا و بحرانی در سیستم‌عامل‌های IOS و IOS XE رفع شده‌اند. علاوه بر این، این شرکت تعدادی توصیه‌ی دیگر را در مورد نقص‌هایی با شدت بالا و متوسط که بر IOS و سایر نرم‌افزارها تاثیر می‌گذارند، منتشر کرده است.

یکی از مهمترین این آسیب‌پذیری‌ها که بحرانی نیز است با شناسه CVE-2020-3205 قابل ردیابی بوده که به یک مهاجم غیرمجاز اجازه می‌دهد تا دستورات شل دلخواه را بر روی یک سرور VDS اجرا کند. مهاجم می‌تواند با ارسال بسته‌های ساخته‌شده‌ی ویژه‌ای به دستگاه قربانی، از این نقص امنیتی بهره ببرد. یک حمله‌ی موفق می‌تواند موجب دسترسی کامل به سیستم شود.

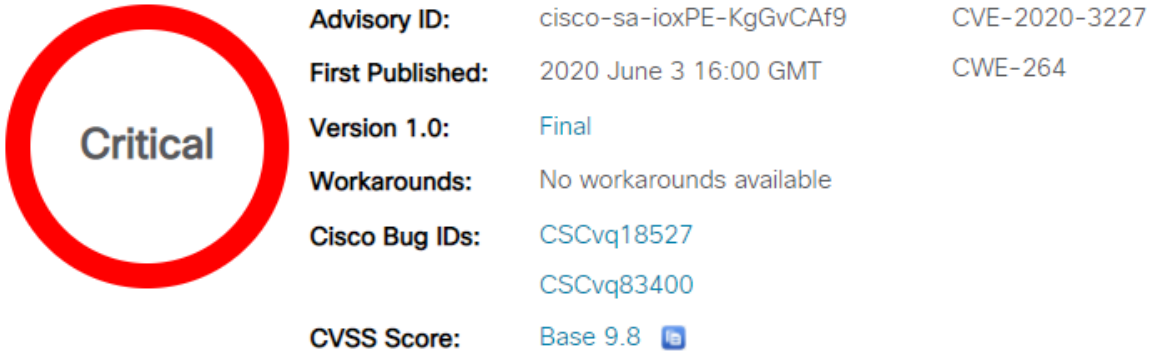
آسیب‌پذیری مهم دیگر با شناسه‌ی CVE-2020-3198 نیز مشابه مورد قبل عمل می‌کند. با توجه به اینکه به یک مهاجم غیرمجاز اجازه می‌دهد تا از راه دور کد دلخواه را بر روی سیستم آسیب‌پذیر اجرا کند، مهاجم قادر است با ارسال بسته‌های مخرب به دستگاه، به سادگی باعث خرابی(crash) و سپس راه‌اندازی مجدد(reboot) دستگاه شود. این موارد همچنین بر روی Cisco ISR 809، ۸۲۹ Industrial Routers و سری ۱۰۰۰ CGR تأثیر می‌گذارند.

جدای از این، سیسکو آسیب‌پذیری با شناسه CVE-2020-3227 را نیز بحرانی اعلام کرده است. به طور خلاصه، با توجه به کسب امتیاز ۹.۸ از ۱۰ در مقیاس CVSS، خطر این آسیب‌پذیری از موارد قبلی کمتر نیست.

شکل ۱. آسیب‌پذیری بحرانی در روترهای سیسکو

۲ آسیب‌پذیری ارتقاء سطح دسترسی با شناسه CVE-2020-3227

در آسیب‌پذیری با شناسه CVE-2020-3227، مسئله کنترل مجوزهای زیرساخت Cisco IOx در Cisco IOS XE مطرح است. این اشکال به یک مهاجم بدون داشتن مجوز و اعتبارنامه اجازه می‌دهد تا به Cisco IOx API دسترسی پیدا کند و دستورات را از راه دور اجرا کند.



شکل ۲. آسیب‌پذیری ارتقاء سطح دسترسی با شناسه CVE-2020-3227

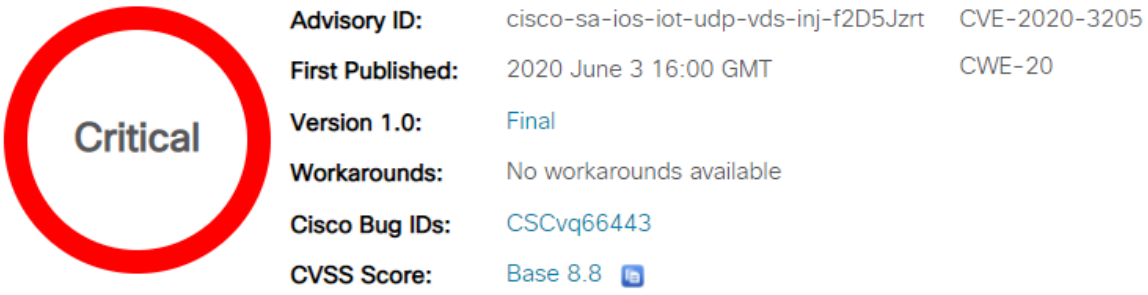
با بررسی انجام شده مشخص شد که IOx به درستی درخواست‌های توکن را بررسی نمی‌کند و در نتیجه، به مهاجم اجازه می‌دهد تا از دستورات ویژه API استفاده کند، یک توکن را درخواست کند و دستورات دلخواه را بر روی دستگاه آلوده، اجرا کند.

علاوه بر این، سیسکو توضیح داده است که به روزرسانی‌های نرم‌افزاری لازم را برای رفع این آسیب‌پذیری منتشر کرده‌است، زیرا هیچ راه‌حلی در دسترس نیست که بتواند این نقص امنیتی را برطرف کند. اگر درمورد محصولاتی که تحت تاثیر این آسیب‌پذیری قرارگرفته‌اند صحبت کنیم، سیسکو قبلا تایید کرده است که نسخه‌ی ۱۶.۳.۱ نرم‌افزار Cisco IOS XE، تحت تاثیر این نقص امنیتی قرار دارد.

۳ آسیب‌پذیری تزریق دستور در VM Channel با شناسه CVE-2020-3205

این نقص امنیتی با شناسه CVE-2020-3205، در VM Channel داخلی نرم‌افزار Cisco IOS برای روترهای Cisco 809، Cisco 829 و Cisco 1000 Series (CGR1000) وجود دارد. این روترها، روترهایی هستند که بر

روی معماری Hypervisor طراحی شده‌اند. این نقص امنیتی می‌تواند به راحتی اجازه دهد مهاجمی غیرمجاز، دستورات شل دلخواه را بر روی VDS دستگاه آلوده اجرا کند.



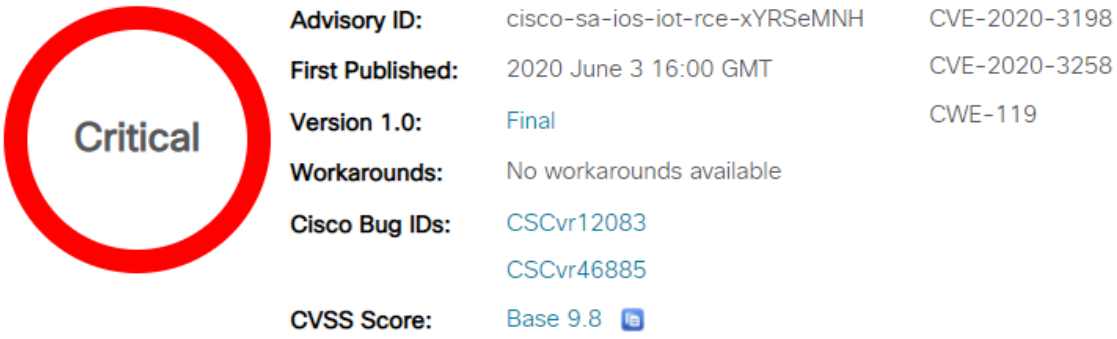
شکل ۳. آسیب‌پذیری تزریق دستور در VM Channel با شناسه CVE-2020-3205

این نقص امنیتی، با ارسال بسته‌های مخرب به قربانی، می‌تواند توسط مهاجم مورد استفاده قرار گیرد. مهاجم با بهره‌برداری موفق از این نقص می‌تواند دستورات دلخواه را با دسترسی روت در محیط شل لینوکس VDS اجرا کند و دسترسی کامل به سیستم را به مهاجم دهد. جدای از این، برای رفع این آسیب‌پذیری، سیسکو به‌روزرسانی‌های نرم‌افزار را منتشر کرده است، زیرا در حال حاضر هیچ راه حلی وجود ندارد که این آسیب‌پذیری را برطرف کند.

همچنین همانطور که خود سیسکو تأیید کرده‌است، این نقص بر روترهای Cisco 809، ۸۲۹ ISR صنعتی و CGR1000 (Cisco 1000 Series Connected Grid Riders) تاثیر گذاشته‌است.

۴ آسیب‌پذیری اجرای کد دلخواه در روترهای صنعتی با شناسه CVE-2020-3198

در آسیب‌پذیری با شناسه CVE-2020-3198، یک خرابی یا راه اندازی مجدد روتر توسط مهاجم ایجاد می‌شود. تمام کاری که لازم است انجام شود این است که بسته های UDP دستکاری‌شده، از طریق IPv4 یا IPv6، به درگاه ۹۷۰۰ فرستاده شوند. سیسکو این آسیب‌پذیری را ۹.۸ از ۱۰ امتیاز، ارزیابی کرده است.



شکل ۴. آسیب‌پذیری اجرای کد دلخواه در روترهای صنعتی با شناسه CVE-2020-3198

همچنین در توصیه‌نامه امنیتی سیسکو، نقص امنیتی با شناسه CVE-2020-3258 امتیاز ۵.۷ را از ۱۰ کسب کرده‌است. با بهره‌برداری از این نقص، مهاجم می‌تواند به شکل کارآمدی کد مخرب را که به یک کاربر محلی با داده‌ی ورود معتبر و با امنیت بالا محدود شده‌است، اجرا کند. این عمل می‌تواند موجب دستکاری حافظه‌ی در حال کار یک دستگاه شود و از روی حافظه‌ی سیستم، رونویسی کند.

جدا از همه‌ی این موارد، این نقص امنیتی بر روی روترهای Cisco 809، ۸۲۹ ISR Industrial، CGR1000 (Cisco 1000 Series Connected Grid Ruters) تأثیر گذاشته است.

سایر آسیب‌پذیری‌ها نیز به عنوان شدید تلقی شده‌اند، زیرا می توانند توسط مهاجمان برای افزایش سطح دسترسی با استفاده از ابزارهای احراز هویت، حملات DoS، اجرای دستورات شل دلخواه و بارگیری تصاویر، از سیستم عامل مخرب استفاده کنند.

با این وجود، برای استفاده از این نقص‌های امنیتی، احراز هویت، دسترسی محلی یا فعالیت توابع غیرفعال شده به طور پیش‌فرض لازم خواهد بود. برخی از آسیب‌پذیری‌های شدید مربوط به IOx است، زیرا آنها به مهاجمان اجازه می‌دهند فایل‌های دلخواه را بنویسند و اصلاح کنند، حملات مستقیم DoS را انجام دهند و کد دلخواه را با دسترسی و مجوز بالا اجرا کنند.

آسیب‌پذیری‌هایی که با شدت متوسط مشخص شده‌اند، بر محصولات صنعتی سیسکو تأثیر می‌گذارند و توسط مهاجمان در حملات XSS قابل استفاده هستند و فایل‌های دلخواه را بازنویسی می‌کنند. سیسکو لیست محصولات تحت تأثیر را منتشر کرده‌است که شامل موارد زیر است:

- Cisco 800 Industrial ISRs
- Cisco 809 Industrial ISRs

- Cisco 829 Industrial ISRs
- CGR1000 (Cisco 1000 Series Connected Grid Routers)
- IC3000 Industrial Compute Gateway
- Industrial Ethernet (IE) 4000 series switches
- Catalyst IE3400 secure series switches
- IR510 WPAN routers

۵ منابع

- https://tools.cisco.com/security/center/publicationListing.x
- https://gbhackers.com/flaws-in-cisco-ios-routers/