بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

آسیب‌پذیری موجود در نرم‌افزار NX-OS

گزارش آسیب‌پذیری

فهرست مطالب

۱ آسیب‌پذیری موجود در نرم‌افزار NX-OS

سیسکو یک نقض با شدت بالا که در نرم‌افزار NX-OS و سیستم‌عامل شبکه که در سوییچ‌های Ethernet سری Nexus سیسکو وجود دارد و می‌تواند باعث حملات انکار سرویس (DoS) شود را وصله کرد. در صورت بهره‌برداری از این آسیب‌پذیری، یک مهاجم احراز هویت نشده از راه دور می‌تواند ورودی‌های لیست کنترل دسترسی (ACL) که در سوئیچ Nexus پیکربندی شده را دور زده و باعث حملات انکار سرویس شود.

طبق توصیه‌های امنیتی سیسکو بهره‌برداری موفقیت‌آمیز می‌تواند باعث شود دستگاه آلوده، بسته IP-in-IP را به طور غیر منتظره رمزگشایی کرده و بسته IP داخلی را ارسال کند. این مسئله باعث می‌شود بسته‌های IP که ورودی ACLهای پیکربندی شده در دستگاه آلوده یا مرزهای امنیتی دیگر را دور می‌زنند، در بخش‌های دیگر شبکه نیز اعمال مخرب خود را انجام دهند.

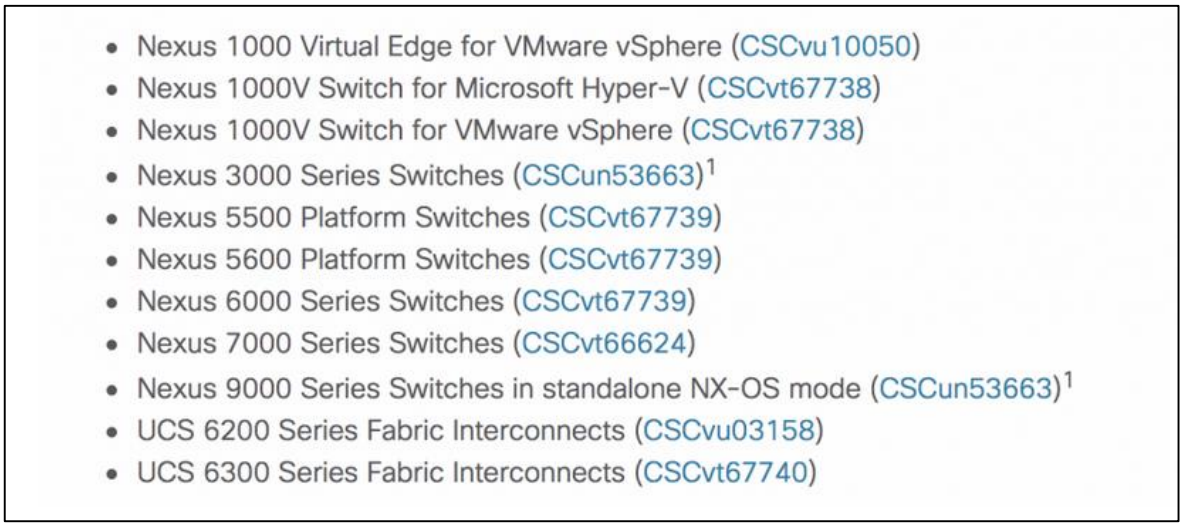
این آسیب‌پذیری (CVE-2020-10136) در پشته شبکه در نرم‌افزار NX-OS سیسکو و در واقع در یک پروتکل tunneling به نام IP-in-IP encapsulation وجود دارد که به بسته‌های IP امکان می‌دهد در یک بسته IP دیگر محصور شوند. این پروتکل در در نرم‌افزار آلوده، بسته‌های IP-in-IP را از هر منبعی (به هر مقصد) بدون پیکربندی صریح بین آدرس‌های IP مبدا و مقصد دریافت می‌کند.

مهاجم می‌تواند با ارسال یک بسته IP-in-IP مخرب به دستگاه آلوده از این مسئله سوءاستفاده کند. به گفته شرکت سیسکو، تحت شرایط خاصی این بسته‌ها می‌توانند باعث فرآیند پشته شبکه، ایجاد اختلال در شبکه، چندین بار راه‌اندازی مجدد سیستم و حملات انکار سرویس در دستگاه‌های آلوده شوند.

۲ دستگاه‌های تحت تأثیر این آسیب‌پذیری

دستگاه‌های تحت تأثیر این نقض، سوئیچ‌های Nexus سری‌های ۱۰۰۰، ۳۰۰۰، ۵۵۰۰، ۵۶۰۰، ۶۰۰۰، ۷۰۰۰ و ۹۰۰۰ و همچنین سیستم محاسبات یکپارچه سیسکو (UCS) سری‌های ۶۲۰۰ و ۶۳۰۰ هستند. کاربران می‌توانند آلوده بودن نرم‌افزار NX-OS را از طریق یک ابزار ذکر شده در توصیه‌های امنیتی سیسکو بررسی کنند.

در صورتی که کاربران از نسخه آسیب‌پذیر نرم‌افزار NX-OS استفاده کنند، محصولات سیسکو موجود در شکل زیر می‌توانند تحت تأثیر این آسیب‌پذیری قرار بگیرند.



شکل ۱

کاربران باید آخرین وصله منتشر شده را اعمال کنند، اگر دستگاهی توانایی غیرفعال کردن IP-in-IP را در پیکربندی خود دارد، توصیه می‌شود در تمام رابط‌هایی که نیازی به این ویژگی ندارند غیرفعال شوند. از سازندگان دستگاه خواسته شده است که IP-in-IP را در پیکربندی پیش‌فرض خود غیرفعال کرده و از مشتریان خود بخواهند که آن را در صورت لزوم پیکربندی کنند.

یک کد PoC برای این آسیب‌پذیری توسط یک محقق امنیتی به نام Yannay Livneh (کاشف این آسیب‌پذیری) منتشر شده است. به گفته این محقق از این کد می‌توان جهت تایید اینکه این دستگاه از پروتکل IP-in-IP encapsulation از منبع تا مقصد دلخواه پشتیبانی می‌کند، استفاده کرد. استفاده از این کد نیازمند حداقل دو دستگاه دیگر با آدرس IP مشخص می‌باشد.

به گفته سیسکو در حال حاضر اطلاعیه عمومی یا استفاده مخرب از این آسیب‌پذیری وجود ندارد. این آسیب‌پذیری با شدت ۸,۶ از ۱۰ و بالا گزارش شده است. این نقض یک هفته پس از اعلام خبر به خطر افتادن سرورهای سیسکو و دو آسیب‌پذیری بحرانی در SaltStack به وجود آمد. این نقض‌ها در چارچوب مدیریت Salt وجود داشته و همچنین در ابزارهای شبکه سیسکو نیز از آن‌ها استفاده می‌شود.

۳ مراجع

[1] https://threatpost.com/cisco-dos-flaw-nexus-switches/156203/