بهره‌برداری هکرها از نقص موجود در نرم‌افزارهای ASA و FTD سیسکو، طی چند ساعت پس از افشای اطلاعات

اخیراً سیسکو یک آسیب‌پذیری بحرانی با شناسه CVE-2020-3452 موجود در نرم افزارهای Adaptive Security Appliance (ASA) و Firepower Threat Defense (FTD) را وصله کرده است.

این آسیب‌پذیری، به یک مهاجم از راه دور این امکان را می‌دهد تا یک حمله‌ی پیمایش دایرکتوری را، که امکان خواندن فایل‌های حساس و مورد هدف قرار دادن سیستم آلوده را فراهم می‌کند، اجرا کند.

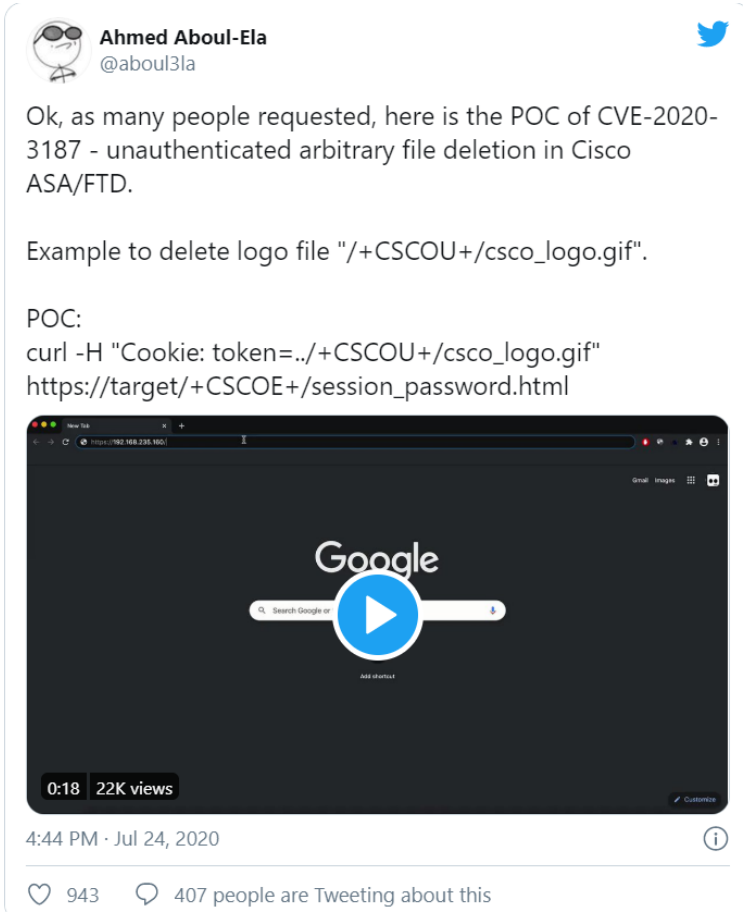
این آسیب‌پذیری به علت عدم اعتبارسنجی URL در درخواست‌های HTTP به وجود آمده است. مهاجم می‌تواند با فرستادن یک درخواست HTTP دستکاری شده که شامل ترتیب کاراکترهای پیمایش دایرکتوری است، از این آسیب‌پذیری بهره‌برداری کند.

بهره‌برداری موفقیت‌آمیز از این آسیب‌پذیری، برای مهاجم امکان مشاهده‌ی هر فایل دلخواه موجود در سیستم‌فایل در دستگاه هدف را، فراهم می‌کند.

سیسکو آپدیت‌های نرم‌افزاری برای برطرف‌کردن این آسیب‌پذیری منتشر کرده است و به کاربرانی که از محصولات تحت‌تاثیر این آسیب‌پذیری استفاده می‌کنند، توصیه کرده است که هرچه سریعتر، محصول خود را به‌روزرسانی کنند.

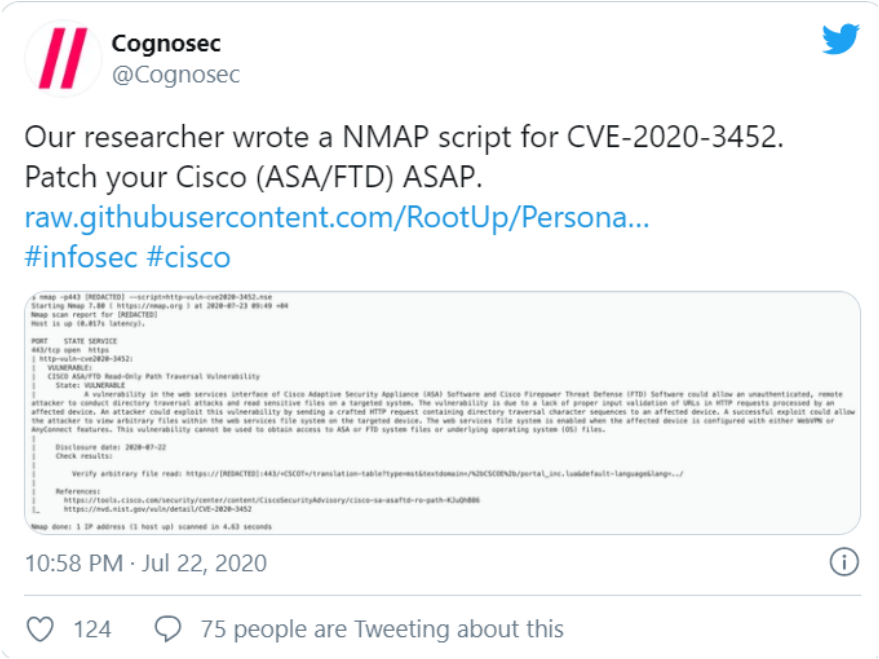
بهره‌برداری از آسیب‌پذیری

این آسیب‌پذیری، توسط میکائیل کلیچنیکوف، از Positive Technologies، و عبدالرحمان نور و احمد عبدالعلی، از RedForce، به سیسکو گزارش داده‌شد.



شکل ۱. توییت عبدالعلی در خصوص آسیب‌پذیری

محقق امنیتی، عبدالعلی، یک کد بهره‌برداری برای این آسیب‌پذیری را در روز ۲۲ ژوئیه، منتشر کرد و محققان Cognosec یک اسکریپت NMAP، برای بهره‌برداری از این نقص، منتشر کردند.



شکل ۲. توییت Cognosec در خصوص بهره‌برداری از آسیب‌پذیری

ساعاتی پس از انتشار کد بهره‌برداری، مهاجمانی موسوم به ET به صورت گسترده شروع به بهره‌برداری از این آسیب‌پذیری کردند. طبق مشاهدات آزمایشگاه Rapid7 تنها حدود ۱۰٪ از دستگاه‌های Cisco ASA/FTD پس از منتشر شدن به‌روزرسانی و وصله‌ای که این مشکل را حل می‌کند، راه‌اندازی مجدد شده‌اند، که این مسئله، به احتمال زیاد، نشان از وصله شدن آسیب‌پذیری آن‌ها است. (تنها ۲۷ مورد از ۳۹۸ شرکت شناسایی شده که در Fortune 500 هستند، به‌روز و راه‌اندازی مجدد شده‌اند.)

با توجه به منتشر شدن کد بهره‌برداری این آسیب‌پذیری و سوءاستفاده گسترده مهاجمان، سیسکو به کاربران و مشتریان خود توصیه کرده است که هرچه سریعتر به‌روزرسانی را انجام دهند.

منبع

https://gbhackers.com/cve-2020-3452-flaw-in-cisco/