بسمه تعالی

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

آسیب‌پذیری Path Traversal در سرویس‌های وب نرم‌افزارهای ASA و FTD سیسکو

خبر آسیب‌پذیری

شناسه سند	MaherReport_13990728-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۵/۲۸
طبقه‌بندی سند	**عادی**

تهران، خیابان شهید بهشتی، نرسیده به خیابان قائم مقام، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ آسیب‌پذیری Path Traversal در سرویس‌های وب نرم‌افزارهای ASA و FTD سیسکو ۱

۱ آسیب‌پذیری Path Traversal در سرویس‌های وب نرم‌افزارهای ASA و FTD سیسکو

آسیب‌پذیری موجود در رابط سرویس‌های وب نرم‌افزارهای Cisco Adaptive Security Appliance (ASA) و Cisco Firepower Threat Defense (FTD)، این امکان را برای مهاجم احراز هویت نشده فراهم می‌آورد تا از راه دور حملات Directory Traversal انجام داده و به فایل‌های حساس سیستم هدف، دسترسی یابد. این آسیب‌پذیری با شناسه CVE-2020-3452 معرفی شده و براساس سیستم امتیاز دهی CVSSv3 دارای امتیاز 7.5 است.

این آسیب‌پذیری، به دلیل اعتبارسنجی نامناسب ورودی URLها در درخواست‌های HTTP رخ می‌دهد. هکرها برای حمله، درخواست‌های HTTP دستکاری شده را که شامل دنباله کاراکترهای پیمایش مسیر (Directory Traversal) می‌باشند به سیستم هدف ارسال می‌کنند. اکسپلویت آسیب‌پذیری، امکان مشاهده اسناد دلخواه هکر را در سیستم هدف فراهم می‌سازد.

آسیب‌پذیری مذکور در صورتی محصولات سیسکو را تحت تأثیر قرار می‌دهد که این محصولات، پیکربندی AnyConnect یا WebVPN را در نسخه آسیب‌پذیر Cisco ASA Software یا Cisco FTD Software استفاده کنند.

زمانی‌که یک دستگاه آسیب‌پذیر با ویژگی WebVPN یا AnyConnect پیکربندی شود، فایل‌سیستم این وب‌سرویس‌ها فعال می‌شود و هکرها می‌توانند به فایل‌سیستم‌ها دسترسی داشته باشند. با این حال، این آسیب‌پذیری نمی‌تواند برای دسترسی به فایل‌های سیستم ASA یا FTD یا فایل‌های سیستم‌عامل استفاده شود. فایل‌های سرویس‌های وب که هکر می‌تواند مشاهده کند ممکن است حاوی اطلاعاتی مانند پیکربندی WebVPN، bookmarkها، کوکی‌های وب، بخشی از محتوای وب و URLهای HTTP باشد.

کاربرانی که از ویژگی SSL Decryption در سنسورهای Cisco Firepower استفاده می‌کنند، می‌توانند با فعال‌سازی اسنورت Rule با استفاده از Firepower Management Center تلاش برای اکسپلوت آسیب‌پذیری را تشخیص داده و بلاک نمایند.

توجه به این نکته الزامیست که سیسکو نسبت به وجود کد اکسپلویت برای این آسیب‌پذیری و تلاش گسترده برای بهره‌برداری از آن هشدار داده است. بنابراین الزامی است تا کاربران هرچه سریع‌تر نسبت به استفاده از نسخه‌های وصله شده اقدام نمایند. نسخه‌های وصله شده نرم‌افزارهای ASA و FTD به ترتیب در جدول‌های ۱ و ۲ معرفی شده‌اند. جدول ۳ نیز جزییات بیشتری در خصوص وصله‌های نرم افزار FTD ارائه می‌دهد.

جدول ۱- نرم افزار ASA سیسکو

سری نسخه Cisco ASA	آخرین نسخه به‌روز شده فاقد آسیب‌پذیری
نسخه قبل از 9.61	استفاده از نسخه‌های بدون آسیب‌پذیری [۱]
9.6	9.6.4.42
9.71	استفاده از نسخه‌های بدون آسیب‌پذیری [۲]
9.8	9.8.4.20
9.9	9.9.2.74
9.10	9.10.1.42
9.12	9.12.3.12
9.13	9.13.1.10
9.14	9.14.1.10

جدول ۲- نرم افزار FDT سیسکو

سری نسخه‌های FTD	آخرین نسخه به‌روز شده فاقد آسیب‌پذیری
پیش‌تر از 6.2.2	آسیب پذیر نیست.
6.2.2	استفاده از نسخه‌های بدون آسیب‌پذیری ۳
6.2.3	6.2.3.16
6.3.0	استفاده از نسخه 6.4.0.9 یا استفاده از نسخه 6.6.0.1 یا استفاده از نسخه 6.3.0.5 یا

[۱] برای این سری از نسخه‌ها آسیب‌پذیری رفع نشده و باید از نسخه‌های فاقد آسیب‌پذیری سری‌های دیگر استفاده شود.
[۲] برای این سری از نسخه‌ها آسیب‌پذیری رفع نشده و باید از نسخه‌های فاقد آسیب‌پذیری سری‌های دیگر استفاده شود.
[۳] برای این سری از نسخه‌ها آسیب‌پذیری رفع نشده و باید از نسخه‌های فاقد آسیب‌پذیری سری‌های دیگر استفاده شود.

	استفاده از نسخه 6.3.0.6 (Fall 2020)
6.4.0	استفاده از نسخه 6.4.0.9 یا استفاده از نسخه 6.4.0.10 (Fall 2020)
6.5.0	استفاده از نسخه 6.6.0.1 یا استفاده از نسخه 6.5.0.4 یا استفاده از نسخه 6.5.0.5 (Fall 2020)
6.6.0	6.6.0.1

جدول ۳- جزئیات بیشتر برخی نسخه ها FTD

نسخه	نام فایل
6.3.0.5	Cisco_FTD_Hotfix_AV-6.3.0.6-3.sh.REL.tar Cisco_FTD_SSP_Hotfix_AV-6.3.0.6-3.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_AV-6.3.0.6-3.sh.REL.tar
6.4.0.9	Cisco_FTD_Hotfix_BM-6.4.0.10-2.sh.REL.tar Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2.sh.REL.tar Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2.sh.REL.tar
6.5.0.4	Cisco_FTD_Hotfix_O-6.5.0.5-3.sh.REL.tar Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3.sh.REL.tar Cisco_FTD_SSP_FP1K_Hotfix_O-6.5.0.5-3.sh.REL.tar Cisco_FTD_SSP_Hotfix_O-6.5.0.5-3.sh.REL.tar

کاربران جهت به‌روزرسانی و ارتقاء به یکی از نسخه‌های وصله شده نرم‌افزار FTD، می‌توانند ازیکی از روش‌های زیر استفاده نمایند.

- برای دستگاه‌هایی که با استفاده از Firepower Management Center (FMC) مدیریت می‌شوند، از رابط FMC برای نصب نسخه وصله شده استفاده کنید. پس از اتمام نصب، سیاست کنترل دسترسی را مجددا اعمال نمایید.
- برای دستگاه‌هایی که با Firepower Device Manager (FDM) مدیریت می‌شوند، از رابط FDM برای نصب نسخه وصله شده استفاده کنید. پس از اتمام نصب، سیاست کنترل دسترسی را مجددا اعمال نمایید.