دو آسیب‌پذیری مهم منتشر شده سیسکو در تاریخ ۹ ژانویه ۲۰۱۹
به همراه راه‌حل‌های آنها

آسیب‌پذیری‌های امنیتی منتشر شده توسط شرکت سیسکو در تاریخ ۹ ژانویه ۲۰۱۹ به همراه راه‌حل:

شرکت سیسکو در این به‌روزرسانی ۱۹ آسیب‌پذیری جدید اشاره کرده‌است. از این تعداد یک آسیب‌پذیری دارای درجه حساسیت بحرانی (Critical) و یک آسیب‌پذیری دارای درجه حساسیت خطرناک (High) و ۱۷ آسیب‌پذیری دارای درجه حسایت متوسط (Medium) می‌باشد. دو آسیب‌پذیری با درجه حساسیت بحرانی و خطرناک مربوط به سرویس امنیتی ایمیل سیسکو می‌باشد که به مدیران شبکه که از این سرویس و نرم‌افزار Cisco AsyncOS استفاده می‌کنند به شدت توصیه می‌شود که به توصیه‌های امنیتی این گزارش توجه کنند و آنها را بر روی دستگاه‌های آسیب‌پذیر خود اعمال کنند.

بحرانی(Critical)	Cisco Email Security Appliance Memory Corruption Denial of Service Vulnerability
عنوان	آسیب‌پذیری منع سرویس از طریق فساد حافظه در سرویس امنیتی ایمیل سیسکو
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۱۵۴۵۳
CVSS Score	Base – ۸.۶
نسخه	۱.۰
شناسه باگ‌های سیسکو	CSCvk۷۳۷۸۶
تاثیر	آسیب‌پذیری منع سرویس (Denial of Service)
تاریخ آخرین به‌روزرسانی	۲۰۱۹ January ۹ ۱۶:۰۰ GMT
توضیحات	آسیب‌پذیری در دو ویژگی Decryption and Verification و Public Key Harvesting در سرویس Secure/Multipurpose Internet Mail Extensions (S/MIME) در نرم‌افزار Cisco AsyncOS برای سرویس امنیتی ایمیل Cisco Email Security Appliance (ESA) به یک مهاجم از راه دور و بدون احراز هویت امکان ایجاد فساد در حافظه سیستم آسیب‌دیده را می‌دهد. بهره‌برداری موفق از این آسیب‌پذیری می‌تواند منجر به بارگذاری مجدد فرایندهای فیلترینگ و در نتیجه حمله منع سرویس[۱] گردد. این آسیب‌پذیری ناشی از اعتبارسنجی نادرست ورودی ایمیل‌های S/MIME-signed است. یک مهاجم با ارسال یک ایمیل S/MIME-signed مخرب از طریق دستگاه هدف می‌تواند از این آسیب‌پذیری سوءاستفاده کند. اگر ویژگی‌های Verification یا Public Key Harvesting تنظیم شده باشد، فرایند فیلترینگ می‌تواند از طریق فساد حافظه و ریستارت موجب شرایط منع سرویس گردد.
محصولات آسیب‌پذیر	تمام نسخه‌های نرم‌افزار AsyncOS برای هر دو نسخه مجازی و سخت‌افزاری Cisco Email Security Appliance (ESA) در صورتیکه برای Decryption و Verification یا S/MIME Public Key Harvesting تنظیم شده باشد، آسیب‌پذیر هستند. مدیر شبکه می‌تواند با طی مراحل زیر تنظیم بودن S/MIME Decryption and Verification را چک کند. ۱. بر روی Mail Policies کلیک کنید و سپس به Mail Flow Policies بروید.

[۱] denial of service (DoS)

۲. تمام سیاست‌های Mail Flow Policies را بررسی کنید.
۳. در هر Mail Flow Policy به بخش Security Features بروید.
۴. فعال بودن گزینه S/MIME Decryption/Verification را بررسی کنید.

مدیر شبکه می‌تواند با طی مراحل زیر تنظیم بودن S/MIME Public Key Harvesting را چک کند.

۱. بر روی Mail Policies کلیک کنید و سپس به Mail Flow Policies بروید.
۲. تمام سیاست‌های Mail Flow Policies را بررسی کنید.
۳. در هر Mail Flow Policy به بخش Security Features بروید.
۴. فعال بودن گزینه S/MIME Public Key Harvesting را بررسی کنید.

برای تعیین اینکه آیا یک نسخه آسیب‌پذیر از نرم افزار AsyncOS سیسکو در یک ESA در حال اجرا است، مدیران شبکه می‌توانند از دستور version در ESA CLI استفاده کنند. مثال زیر نشان دهنده خروجی این فرمان است که نشان می‌دهد نسخه ۱۰.۰.۱-۰۸۷ این نرم‌افزار در حال اجرا است.

ciscoesa> **version**

Current Version

==========

Product: Cisco C۱۰۰V Email Security Virtual Appliance
Model: C۱۰۰V
Version: **۱۰.۰.۱-۰۸۷**

نکته: برای اطلاعات بیشتر در مورد قابلیت‌ها و تنظیمات ESA S / MIME لطفا به لینک زیر مراجعه کنید.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa110/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010011.html#con_1127154

راه حل

در جدول زیر، ستون سمت چپ لیستی از نسخه‌های مهم نرم‌افزار AsyncOS برای ESA را نشان می‌دهد. ستون سمت راست نشان می‌دهد که آیا این نسخه‌های آسیب‌پذیر و اولین نسخه پچ شده را نشان می‌دهد.

مدیران شبکه باید نرم‌افزار AsyncOS را مطابق جدول زیر به نسخه مناسب ارتقاء دهند.

Cisco AsyncOS Software for ESA Major Release	First Fixed Release
Prior to 9.0	Affected; migrate to 11.0.2-044
9.0.x	Affected; migrate to 11.0.2-044
10.0.x	Affected; migrate to 11.0.2-044
11.0.x	11.0.2-044
11.1.x	11.1.1-037 or 11.1.2-023
12.x	Not vulnerable

۱. آخرین نسخه این نرم‌افزار را دانلود کنید.
۲. دو ویژگی Decryption and Verification و Public Key Harvesting را در سرویس S/MIME غیرفعال کنید.

خطرناک(High)	Cisco Email Security Appliance URL Filtering Denial of Service Vulnerability
عنوان	آسیب‌پذیری منع سرویس از طریق URL Filtering در سرویس امنیتی ایمیل سیسکو
شناسه آسیب‌پذیری	CVE-۲۰۱۸-۱۵۴۶۰
CVSS Score	Base – ۸.۶
نسخه	۱.۰
شناسه باگ‌های سیسکو	CSCvm۸۱۶۲۷
تاثیر	آسیب‌پذیری منع سرویس (Denial of Service)
تاریخ انتشار	۲۰۱۹ January ۹ ۱۶:۰۰ GMT
توضیحات	آسیب‌پذیری در ویژگی فیلترینگ پیام ایمیل در نرم‌افزار Cisco AsyncOS برای سرویس امنیتی ایمیل Cisco Email Security Appliance (ESA) به یک مهاجم از راه دور و بدون احراز هویت اجازه می‌دهد تا با افزایش استفاده از cpu تا ۱۰۰ درصد موجب حمله منع سرویس گردد. این آسیب‌پذیری ناشی از فیلترینگ نادرست پیام‌های ایمیل است که حاوی مراجع به آدرس‌های لیست سفید[۲] هستند. یک مهاجم با ارسال یک ایمیل مخرب که شامل تعداد زیادی آدرس‌های لیست سفید است می‌تواند از این آسیب‌پذیری سوءاستفاده کند. با سوءاستفاده از این آسیب‌پذیری مهاجم قادر به اجرای حمله منع سرویس و درنتیجه متوقف کردن فرایندهای اسکن و فوروارد پیام‌های ایمیل می‌شود.
محصولات آسیب‌پذیر	تمام نسخه‌های نرم‌افزار AsyncOS برای هر دو نسخه مجازی و سخت‌افزاری Cisco Email Security Appliance (ESA) در صورتیکه برای ویژگی URL Filtering as Global Setting فعال باشد (به صورت پیش‌فرض این ویژگی غیرفعال است) و لیست سفید URLهای مورد استفاده، آسیب‌پذیر هستند. برای تعیین اینکه آیا یک نسخه آسیب‌پذیر از نرم افزار AsyncOS سیسکو در یک ESA در حال اجرا است، مدیران شبکه می‌توانند از دستور version در ESA CLI استفاده کنند. مثال زیر نشان دهنده خروجی این فرمان است که نشان می‌دهد نسخه ۱۰.۰.۱-۰۸۷ این نرم‌افزار در حال اجرا است. ciscoesa> **version** Current Version ==========

[۲] whitelisted URLs

	Product: Cisco C۱۰۰V Email Security Virtual Appliance Model: C۱۰۰V Version: **۱۰.۰.۱-۰۸۷** برای بررسی اینکه آیا Cisco ESA با ویژگی URL Filtering پیکربندی شده و از لیست سفید URLها استفاده می‌کند می‌توانید به مسیر GUI > Security Services > URL Filtering بروید. در اینجا اگر گزینه URL Category and Reputation Filters فعال باشد و URL whitelist با مقدار هیچ (None) مقداردهی شده باشد آنگاه این دستگاه آسیب‌پذیر خواهد بود.
راه حل	دو راه حل ممکن برای حل این آسیب‌پذیری وجود دارد: راه‌حل اول: اگر Global URL Filtering مورد نیاز نیست، مدیران شبکه می‌توانند با پیروی از مراحل زیر آن‌را غیرفعال کنند: ۱. در ESA مسیر Security Services > URL Filtering را دنبال کنید. ۲. بر روی Edit Global Settings کلیک کنید و مقدار none را برای Use a URL whitelist انتخاب کنید. با این کار global whitelist غیرفعال می‌شود. راه‌حل دوم: اگر ویژگی URL Filtering موردنیاز است بعد از غیرفعال کردن Global URL Filtering همانطور که در راه‌حل اول توضیح داده شد، مدیران شبکه می‌توانند یک محدوده معتبر URL مشخص یا یک مجموعه URL را برای اعمال whitelist از طریق Content Filter انتخاب کنند. برای این‌کار باید مراحل زیر را طی کنید. ۱. در ESA مسیر Mail Policies > Incoming Content Filters را دنبال کنید. ۲. یک Content Filter جدید با کلیک بر روی Add Filter ایجاد کنید (اختیاری). ۳. بر روی Content Filter موردنظر کلیک کنید و مسیر **Add Action > URL Reputation > Select Custom Range** را دنبال کنید. ۴. رنج مورد نظر را وارد کنید. ۵. فعالیت‌های **Add Action > URL Categories > Add desired Categories set** را به ترتیب دنبال کنید. ۶. Whitelist موردنظر را انتخاب کنید. ۷. بر روی Submit > OK کلیک کنید. در جدول زیر، ستون سمت چپ لیستی از نسخه‌های مهم نرم‌افزار AsyncOS برای ESA را نشان می‌دهد. ستون سمت راست نسخه‌های آسیب‌پذیر و اولین نسخه پچ شده را نشان می‌دهد.

مدیران شبکه باید نرم‌افزار AsyncOS را مطابق جدول زیر به نسخه مناسب ارتقاء دهند.

Cisco AsyncOS Software for ESA Major Release	First Fixed Release
Prior to 9.0	Affected; migrate to 11.0.2-044 MD
9.0.x	Affected; migrate to 11.0.2-044 MD
10.0.x	Affected; migrate to 11.0.2-044 MD
11.0.x	11.0.2-044 MD
11.1.x	11.1.2-023 MD
12.x	Not affected

در ادامه لیستی از آسیب‌پذیری‌های با درجه حساسیت متوسط که شرکت سیسکو در تاریخ ۹ ژانویه ۲۰۱۹ منتشر کرده نشان داده شده‌است.

شناسه آسیب‌پذیری	عنوان آسیب‌پذیری
CVE-۲۰۱۸-۱۵۳۹۳	Cisco Content Security Management Appliance Cross-Site Scripting Vulnerability
CVE-۲۰۱۸-۱۵۴۶۴	Cisco ASR ۹۰۰ Series Aggregation Services Router Software Denial of Service Vulnerability
CVE-۲۰۱۸-۱۵۴۵۷	Cisco Prime Infrastructure Cross-Site Scripting Vulnerability
CVE-۲۰۱۸-۱۵۴۶۶	Cisco Policy Suite Graphite Unauthenticated Read-Only Access Vulnerability
CVE-۲۰۱۸-۰۱۸۱	Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent Software Redis Server Unauthenticated Access Vulnerability
CVE-۲۰۱۸-۰۴۷۴	Cisco Unified Communications Manager Digest Credentials Disclosure Vulnerability
CVE-۲۰۱۸-۱۵۴۵۸	Cisco Firepower Management Center Disk Utilization Denial of Service Vulnerability
CVE-۲۰۱۸-۰۴۸۴	Cisco IOS and IOS XE Software Secure Shell Connection on VRF Vulnerability
CVE-۲۰۱۸-۱۵۴۴۰ CVE-۲۰۱۸-۱۵۴۶۳	Cisco Identity Services Engine Multiple Cross-Site Scripting Vulnerabilities

CVE-۲۰۱۸-۱۵۴۵۶	Cisco Identity Services Engine Password Recovery Vulnerability
CVE-۲۰۱۸-۰۴۴۹	Cisco Jabber Client Framework Insecure Directory Permissions Vulnerability
CVE-۲۰۱۸-۰۴۸۳	Cisco Jabber Client Framework Instant Message Cross-Site Scripting Vulnerability
CVE-۲۰۱۸-۰۴۶۱	Cisco IP Phone ۸۸۰۰ Series Arbitrary Script Injection Vulnerability
CVE-۲۰۱۸-۰۴۸۲	Cisco Prime Network Control System Stored Cross-Site Scripting Vulnerability
CVE-۲۰۱۸-۰۲۸۲	Cisco IOS and IOS XE Software TCP Denial of Service Vulnerability
CVE-۲۰۱۸-۱۵۴۶۷	Cisco TelePresence Management Suite Cross-Site Scripting Vulnerability
CVE-۲۰۱۸-۱۵۴۶۱	Cisco Webex Business Suite Cross-Site Scripting Vulnerability

مراجع

https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities