مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش اصلاحیه امنیتی (۲) محصولات سیسکو با حساسیت Critical در سپتامبر ۲۰۱۹

شرکت Cisco یکی از بزرگترین تولیدکنندگان تجهیزات نرم‌افزاری و سخت‌افزاری شبکه می باشد که با توجه به پیشرفت روز افزون حوزه فناوری اطلاعات و به موازات آن افزایش چشم‌گیر تهدیدات سایبری در سطح جهان و آسیب‌پذیری‌های موجود در این تجهیزات می‌تواند موجب به خطر افتادن اطلاعات کاربران شود. از این رو بخش‌های مختلف Cisco به صورت مداوم و چندین مرتبه در ماه اقدام به ارائه آسیب‌پذیری‌های کشف شده در سرویس‌ها و تجهیزات این شرکت کرده و راه‌حل‌هایی برای رفع این آسیب‌پذیری‌ها ارائه می‌کنند. در این گزارش محصولاتی که دارای آسیب‌پذیری با سطح (Critical) هستند و می‌توان با مراجعه به لینک مشخص شده اطلاعات جامع در مورد آسیب‌پذیری و نحوه رفع آن را کسب کرد.

Cisco Data Center Network Manager Authentication Bypass Vulnerability	**بحرانی(Critical)**
آسیب‌پذیری دور زدن احراز هویت مدیر شبکه مرکز داده سیسکو	عنوان
CVE-2019-1619	شناسه آسیب‌پذیری
Base 9.8	CVSS Score
Final 1.1	نسخه
CSCvo64641	شناسه باگ‌های سیسکو
Authentication Bypass Vulnerability	تاثیر
2019 September 19 16:08 GMT	تاریخ آخرین به‌روزرسانی
این آسیب‌پذیری در رابط مدیریت وب، مدیر شبکه‌ای مرکز داده سیسکو، می‌تواند به یک مهاجم غیرمجاز این دسترسی را بدهد که بدون احراز هویت اقدامات دلخواه را با امتیازات Administrative Privileges بر روی یک دستگاه آسیب اجرا کند.	توضیحات
Cisco Data Center Network Manager (DCNM) software releases prior to Release 11.1	محصولات آسیب‌پذیر
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-bypass	راه حل

Cisco Data Center Network Manager Arbitrary File Upload and Remote Code Execution Vulnerability	**بحرانی(Critical)**
آسیب‌پذیری اجرای کد از راه دور و بارگذاری فایل دلخواه در مدیر شبکه مرکز داده سیسکو	عنوان
CVE-2019-1620	شناسه آسیب‌پذیری
Base 9.8	CVSS Score
Final 1.1	نسخه
CSCvo64647	شناسه باگ‌های سیسکو
Remote Code Execution	تاثیر
2019 September 19 16:08 GMT	تاریخ آخرین به‌روزرسانی
یک آسیب‌پذیری در رابط مدیریت وب، مدیر شبکه‌ای مرکز داده سیسکو، می‌تواند به یک مهاجم غیرمجاز این دسترسی را بدهدکه فایل‌های دلخواه را بر روی یک دستگاه آسیب‌پذیر اجرا کند.	توضیحات
Cisco Data Center Network Manager (DCNM) software releases prior to Release 11.1	محصولات آسیب‌پذیر
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-codex	راه حل

Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability	**بحرانی(Critical)**
آسیب‌پذیری DOS وب سرویس‌های Adaptive Security Appliance سیسکو	عنوان
CVE-2018-0296	شناسه آسیب‌پذیری
Base 8.6	CVSS Score
Final 1.4	نسخه
CSCvi16029	شناسه باگ‌های سیسکو
Denial of Service	تاثیر
2019 September 24 17:49 GMT	تاریخ آخرین به‌روزرسانی
یک آسیب‌پذیری در رابط وب Cisco Adaptive Security Appliance (ASA) می‌تواند به یک مهاجم از راه دور این اجازه را بدهد که بدون احراز هویت یک دستگاه آسیب دیده را بارگذاری مجدد کند در نتیجه منجر به منع سرویس می شود. همچنین در بعضی نسخه‌های خاص از ASA ممکن است که بارگذاری مجدد نشود اما یک مهاجم می‌تواند اطلاعات حساس سیستم را بدون تایید اعتبار با استفاده از تکنیک Directory Traversal بدون احراز هویت مشاهده کند.	توضیحات
این آسیب‌پذیری بر نرم‌افزار Cisco ASA و Cisco Firepower Threat Defence (FTD) که روی محصولات زیر سیسکو اجرا می شود، تأثیر می‌گذارد: 3000 Series Industrial Security Appliance (ISA) ASA 1000V Cloud Firewall ASA 5500 Series Adaptive Security Appliances ASA 5500-X Series Next-Generation Firewalls ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers Adaptive Security Virtual Appliance (ASAv) Firepower 2100 Series Security Appliance Firepower 4100 Series Security Appliance Firepower 9300 ASA Security Module FTD Virtual (FTDv)	محصولات آسیب‌پذیر

راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd