بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

گزارش آسیب‌پذیری‌های منتشر شده سیسکو در ماه می ۲۰۱۸

در این گزارش مشکلات امنیتی منتشر شده توسط شرکت سیسکو در ماه می ۲۰۱۸ و آسیب‌پذیری‌ها به همراه راه حل آنها ارائه شده است. شرکت سیسکو در آخرین آپدیت‌ها و معرفی آسیب‌پذیری‌ها به ۲۹ آسیب‌پذیری جدید اشاره کرده است. از این تعداد ۵ آسیب‌پذیری دارای درجه حساسیت بحرانی (Critical) و ۹ آسیب‌پذیری دارای درجه حساسیت خطرناک(High) و ۱۵ آسیب‌پذیری دارای درجه حسایت متوسط (Medium) می‌باشد. در این گزارش آسیب‌پذیری‌های مهم ماه می ۲۰۱۸ شرح داده شده‌اند.

بحرانی (Critical)	Cisco WebEx Advanced Recording Format Remote Code Execution Vulnerability
عنوان	فرمت ذخیره‌سازی Webex در سیسکو با آسیب‌پذیری اجرای کد از راه دور
شناسه آسیب‌پذیری	CVE-2018-0264
CVSS Score	Base - 9.6
نسخه	1.0
شناسه باگ‌های سیسکو	CSCvh85410 CSCvh85430 CSCvh85440 CSCvh85442 CSCvh85453 CSCvh85457
تاثیر	اجرای کد از راه دور(Remote Code Execution)
تاریخ انتشار	2018 May 2 16:00 GMT
توضیحات	سرویس‌های Cisco WebEx Business Suite (WBS) امکان برقراری جلسات به صورت چندرسانه‌ای را در سراسر جهان برای افراد فراهم می‌کند که توسط Cisco WebEx مدیریت و نگهداری می شود. این سرویس‌ها باعث می‌شود هر فردی بتواند بدون حضور فیزیکی در جلسات یا کنفرانس‌ها شرکت داشته‌باشد. فرمت فایل ARF برای ذخیرسازی جلسات WebEx که در یک وب‌سایت جلسات WebEx یا در کامپیوتر شرکت‌کننده ضبط شده است مورد استفاده قرار می‌گیرد. Cisco WebEx ARF Player یک برنامه کاربردی است که برای بازپخش و ویرایش فایل‌های ذخیره شده WebEx ARF (فایل‌های با فرمت arf.) مورد استفاده قرار می‌گیرد. این برنامه می‌تواند به صورت خودکار حین دسترسی کاربر در سایت Cisco WebEx Meetings به فایل ذخیره شده نصب گردد. همچنین می‌توان به صورت دستی آن را از طریق لینک https://www.webex.com/play-webex-recording.html نصب کرد. یک آسیب‌پذیری در Cisco WebEx Network Recording Player (سرویس برگزاری کنفرانس تحت وب) برای فایل‌های با فرمت Advanced Recording Format (ARF) می‌تواند به یک مهاجم ناشناخته امکان اجرای کد دلخواه از راه دور در سیستم یک کاربر را فراهم نماید.

	یک مهاجم می تواند از این آسیب پذیری با ارسال یک لینک یا پیوست ایمیل شامل یک فایل ARF مخرب به کاربر و باز کردن آن توسط کاربر بهره برداری کند. بهره برداری موفق از این آسیب‌پذیری می‌تواند مهاجم را مجاز به اجرای کد دلخواه در سیستم کاربر کند. شرکت سیسکو نسخه‌های متاثر از این آسیب‌پذیری را در سایت برای Cisco WebEx Business Suite meeting Cisco WebEx Meetings و Cisco WebEx Meetings Server و همچنین Cisco WebEx ARF Player را برای رسیدگی به این آسیب پذیری به روز رسانی کرده است.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی سایت‌های Cisco WebEx Business Suite Cisco WebEx Meetings سرور Cisco WebEx Meetings و پخش‌کننده Cisco WebEx ARF تاثیر داشته است. سرویس‌گیرنده‌های (WBS31 and WBS32) که از نسخه‌های زیر استفاده می‌کنند تحت تاثیر این آسیب‌پذیری قرار دارند. • Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.4 • Cisco WebEx Business Suite (WBS32) client builds prior to T32.12 • Cisco WebEx Meetings with client builds prior to T32.12 • Cisco WebEx Meeting Server builds prior to 3.0 Patch 1 برای اطمینان از اینکه سایت Cisco WebEx meeting یک نسخه آسیب‌پذیر از را اجرا می‌کند کاربران می‌توانند به حساب خود در سایت Cisco WebEx meeting وارد شده و به قسمت Support > Downloads مراجعه کنند. نسخه سرویس گیرنده WebEx در سمت راست صفحه زیر About Meeting Center نمایش داده خواهد شد. به‌روزرسانی‌های نرم‌افزار Cisco WebEx در client builds جمع‌آوری شده است. به عنوان مثال سرویس‌گیرنده build 30.32.16 به build 30.32.17 به‌روزرسانی گردد.
راه حل	برای حل این مشکل باید ابتدا کل ابزار WebEx را حذف کرد که این عمل در سیستم عامل مایکروسافت از طریق ابزار Meeting Services Removal Tool و در سیستم عامل مکینتاش از طریق ابزار Mac WebEx Meeting Application Uninstaller قابل انجام است. برای دانلود این ابزارها نیز می‌توانید به لینک زیر مراجعه کنید. **https://collaborationhelp.cisco.com/article/en-us/WBX000026396** برای حذف نرم‌افزار در سیستم عامل لینوکس می‌توانید راهنمایی‌های لازم را در لینک زیر دریافت کنید. **https://collaborationhelp.cisco.com/article/en-us/WBX000026396** سیسکو به‌روزرسانی‌های این نرم‌افزار را که به این آسیب‌پذیری اشاره دارد به صورت رایگان منتشر کرده است. کاربران فقط می‌توانند نرم‌افزاری را که قبلا خریداری کرده‌اند و لایسنس معتبر آن را دارند دانلود کنند.

Cisco Prime File Upload Servlet Path Traversal and Remote Code Execution Vulnerability	بحرانی(Critical)
آسیب‌پذیری اجرای کد از راه دور در سرویس سیسکو Prime File Upload Servlet Path Traversal	عنوان
CVE-2018-0258	شناسه آسیب‌پذیری
Base - 9.8	CVSS Score
1.1	نسخه
CSCvf32411 CSCvf81727	شناسه باگ‌های سیسکو
اجرای کد از راه دور(Remote Code Execution)	تاثیر
2018 May 2 16:00 GMT	تاریخ انتشار
یک آسیب‌پذیری در File Upload servlet در محصول Data Center Network Manager (DCNM) سیسکو می‌تواند برای یک مهاجم از راه دور امکان بارگذاری فایل‌های دلخواه خود در هر پوشه‌ای از یک دستگاه آسیب‌پذیر و همچنین اجرای آن فایل‌ها را فراهم می‌کند. این آسیب‌پذیری ناشی از اعتبارسنجی نامناسب ورودی پارامترهای موجود در درخواست HTTP و یک خطای پردازش در مکانیزم کنترل دسترسی نقش-محور (RBAC) در URL ها می‌باشد. مهاجمی می‌تواند از طریق بهره‌برداری از این آسیب‌پذیری و با استفاده از تکنیک پیمایش مسیر یک فایل Java Server Pages (JSP) را در یک فولدر خاص بارگذاری و سپس آن فایل را از راه دور اجرا کند. درجه CVSS برای این آسیب‌پذیری: 9.8 سطح امنیتی این آسیب‌پذیری: Critical شناسه باگ سیسکو برای این آسیب‌پذیری: CSCvf32411 یک آسیب‌پذیری در File Upload servlet در محصول Data Center Network Manager (DCNM) سیسکو می‌تواند برای یک مهاجم از راه دور امکان بارگذاری فایل‌های دلخواه خود در هر پوشه‌ای از یک دستگاه آسیب‌پذیر و همچنین اجرای آن فایل‌ها را فراهم می‌کند. این آسیب‌پذیری ناشی از اعتبارسنجی نامناسب ورودی پارامترهای موجود در درخواست HTTP و یک خطای پردازش در مکانیزم کنترل دسترسی نقش-محور (RBAC) در URL ها می‌باشد. مهاجمی می‌تواند از طریق بهره‌برداری از این آسیب‌پذیری و با استفاده از تکنیک پیمایش مسیر یک فایل Java Server Pages (JSP) را در یک فولدر خاص بارگذاری و سپس آن فایل را از راه دور اجرا کند. درجه CVSS برای این آسیب‌پذیری: 8.8 سطح امنیتی این آسیب‌پذیری: High	توضیحات

	شناسه باگ سیسکو برای این آسیب‌پذیری: CSCvf81727
محصولات آسیب‌پذیر	محصولات زیر تحت تاثیر این آسیب‌پذیری قرار دارند: • Cisco Prime Data Center Network Manager (DCNM) - Version 10.0 and later • Cisco Prime Infrastructure (PI) - All versions
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری در دستگاه مورد تهاجم را دانلود نمایید.

بحرانی(Critical)	Cisco Secure Access Control System Remote Code Execution Vulnerability
عنوان	آسیب‌پذیری اجرای کد از راه دور در سیستم کنترل دسترسی از راه دور امن سیسکو (ACS)
شناسه آسیب‌پذیری	CVE-2018-0253
CVSS Score	Base - 9.8
نسخه	1.0
شناسه باگ‌های سیسکو	CSCve69037
تاثیر	اجرای کد از راه دور(Remote Code Execution)
تاریخ انتشار	2018 May 2 16:00 GMT
توضیحات	سیستم کنترل دسترسی امن سیسکو ACS به عنوان یک سرور RADIUS و +TACACS عمل می‌کند که شامل احراز هویت کاربر کنترل دسترسی کاربر و administrator دستگاه و کنترل Policy است. ACS یک مدیریت مرکزی برای سیاست‌های دسترسی مدیریت دستگاه سیاست‌های دسترسی شبکه بی‌سیم شبکه سیمی 802.1x و VPN از راه دور را فراهم می‌کند. سرویس ACS اطلاعات شناسایی را از یک پایگاه داده خارجی بازیابی می‌کند. یک آسیب‌پذیری در ACS می‌تواند به یک مهاجم امکان اجرای دستورات دلخواه از راه دور در یک سیستم آسیب‌دیده را فراهم کند. دستورات مهاجم در سطح دسترسی کاربر اجرا می‌شوند. این آسیب پذیری ناشی از اعتبارسنجی نامناسب در پروتکل Action Message Format (AMF) است. مهاجم می‌تواند با ارسال یک پیام AMF ساخته شده حاوی کد مخرب به کاربر هدف از این آسیب پذیری بهره برداری کند. یک سوءاستفاده می‌تواند به مهاجم اجازه دهد دستورات دلخواه خود را بر روی دستگاه ACS اجرا کند. سیسکو به روز رسانی‌های نرم افزاری مربوط به این آسیب پذیری است منتشر کرده است.

محصولات آسیب‌پذیر	تمام محصولات ACS تا نسخه 5.8 و پچ 7 تحت تاثیر این آسیب‌پذیری قرار دارند. سرپرست‌های شبکه می‌توانند به دو روش زیر نسخه اجرایی سرویس ACS بر روی یک دستگاه تشخیص دهند. ۱- Cisco Secure ACS CLI شما می‌توانید در Cisco Secure ACS CLI با استفاده از دستور show version نسخه اجرایی سرویس ACS را مشاهده کنید. acs55/admin# **show version** Cisco Application Deployment Engine OS Release: 2.2 ADE-OS Build Version: 2.2.2.013 ADE-OS System Architecture: x86_64 Copyright (c) 2005-2015 by Cisco Systems, Inc. All rights reserved. Hostname: acsx5 Version information of installed applications --- Cisco ACS VERSION INFORMATION --- Version : 5.8.0.32 Internal Build ID : B.442 Patches : 5-8-0-32-1 acs55/admin# ۲- رابط‌کاربری مبتنی بر وب Cisco Secure ACS ابتدا در رابط‌کاربری مبتنی بر وب Cisco Secure ACS لاگین کنید و سپس بر روی گزینه About در بالای صفحه گوشه سمت راست کلیک کنید. اطلاعاتی در رابطه با این سرویس مشاهده خواهید کرد.
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

Cisco WebEx Clients Remote Code Execution Vulnerability	بحرانی (Critical)
آسیب‌پذیری اجرای کد از راه دور در کلاینت‌های Cisco WebEx	عنوان
CVE-2018-0112	شناسه آسیب‌پذیری
Base - 9.0	CVSS Score
1.3	نسخه
CSCvg19384 CSCvi10746	شناسه باگ‌های سیسکو
اجرای کد از راه دور(Remote Code Execution)	تاثیر
2018 May 2 14:08 GMT	تاریخ به‌روزرسانی
سرویس‌های Cisco WebEx Business Suite (WBS) امکان برقراری جلسات به صورت چندرسانه‌ای را در سراسر جهان برای افراد فراهم می‌کند که توسط Cisco WebEx مدیریت و نگهداری می شود. این سرویس‌ها باعث می‌شود هر فردی بتواند بدون حضور فیزیکی در جلسات یا کنفرانس‌ها شرکت داشته‌باشد. Cisco WebEx Business Suite شامل Cisco WebEx Event Center Cisco WebEx Meeting Center Cisco WebEx Support Center و Cisco WebEx Training Center می‌باشد. یک آسیب‌پذیری در Cisco WebEx Business Suite meeting Cisco WebEx Meetings و Cisco WebEx Meetings Server می‌تواند به یک مهاجم ناشناخته امکان اجرای کد دلخواه از راه دور در سیستم یک کاربر را فراهم نماید. این آسیب‌پذیری ناشی از اعتبارسنجی ورودی نامناسب کلاینت‌های Cisco WebEx است. یک مهاجم می‌تواند در یک جلسه با استفاده از ارسال مستقیم یک فایل فلش با پسوند(swf.) به کاربران از طریق قابلیت به اشتراک‌گذاری فایل در این نرم‌افزار از این آسیب‌پذیری بهره‌برداری کند.	توضیحات

محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی کلاینت‌هایی که نرم‌افزار WebEx meeting بر روی آنها نصب باشد تاثیرگذار است. نسخه‌هایی که تحت تاثیر این آسیب‌پذیری هستند در لیست زیر آورده شده‌است. • Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.2 • Cisco WebEx Business Suite (WBS32) client builds prior to T32.10 • Cisco WebEx Meetings with client builds prior to T32.10 • Cisco WebEx Meetings Server builds prior to 2.8 MR2 برای اطمینان از اینکه سایت Cisco WebEx Business Suite یک نسخه آسیب‌پذیر از را اجرا می‌کند کاربران می‌توانند به حساب خود در سایت Cisco WebEx meeting وارد شده و به قسمت **Support** > **Downloads** مراجعه کنند. نسخه کلاینت WebEx در سمت راست صفحه زیر About Meeting Center نمایش داده شده‌است.
راه حل	برای حل این مشکل باید ابتدا کل ابزار WebEx را حذف کرد که این عمل در سیستم عامل مایکروسافت از طریق ابزار Meeting Services Removal Tool و در سیستم عامل مکینتاش از طریق ابزار Mac WebEx Meeting Application Uninstaller قابل انجام است. برای دانلود این ابزارها نیز می‌توانید به لینک زیر مراجعه کنید. https://collaborationhelp.cisco.com/article/en-us/WBX000026396 برای حذف نرم‌افزار در سیستم عامل لینوکس می‌توانید راهنمایی‌های لازم را در لینک زیر دریافت کنید. https://collaborationhelp.cisco.com/article/en-us/WBX000026396 سیسکو به‌روزرسانی‌های این نرم‌افزار را که به این آسیب‌پذیری اشاره دارد به صورت رایگان منتشر کرده‌است. کاربران فقط می‌توانند نرم‌افزاری را که قبلا خریداری کرده‌اند و لایسنس معتبر آن را دارند دانلود کنند.

بحرانی (Critical)	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability
عنوان	آسیب‌پذیری اجرای کد از راه دور در ویژگی (Smart Install) نصب هوشمند Cisco IOS و IOS XE
شناسه آسیب‌پذیری	CVE-2018-0171
CVSS Score	Base - 9.8
نسخه	1.7 Final
شناسه باگ‌های	CSCvg76186

سیسکو	
تاثیر	اجرای کد از راه دور(Remote Code Execution)
تاریخ به‌روزرسانی	2018 May 3 19:35 GMT
توضیحات	ویژگی Smart Install در تجهیزات سیسکو بمنظور پیکربندی plug-and-play و ویژگی مدیریت تصویر به وجود آمده است که به مدیران اجازه می‌دهد تا بتوانند به راحتی سوییچ‌های شبکه مشتریان را پیاده‌سازی کنند. این آسیب‌پذیری در ویژگی Smart Install نرم‌افزار سیسکو IOS و IOS XE می‌تواند به یک مهاجم مجوز دسترسی به یک دستگاه آسیب‌دیده را برای حمله DOS یا اجرای کد دلخواه از راه دور را دهد. مهاجم می‌تواند با ارسال یک پیام Smart Install بر روی پورت TCP 4786 به یک دستگاه آسیب‌دیده از این آسیب‌پذیری بهره‌برداری کند. مهاجم می‌تواند با سواستفاده از سرریز بافر تاثیرات زیر را بر روی دستگاه داشته باشد: • راه اندازی مجدد دستگاه • اجرای کد دلخواه بر روی دستگاه • ایجاد یک حلقه(loop) نامحدود در دستگاه ویژگی Smart Install بطور پیش‌فرض بر روی سوییچ‌هایی که نسخه نرافزار سیسکو IOS را اجرا می‌کنند هنوز به‌روزرسانی نشده است.
محصولات آسیب‌پذیر	دستگاه‌هایی که نسخه‌های آسیب‌پذیر نرم‌افزار سیسکو IOS یا IOS XE بر روی آنها در حال اجراست و ویژگی Smart Install در آنها فعال است تحت تاثیر این آسیب‌پذیری هستند. سوییچ‌هایی که نسخه‌های پیش از 12.2(52)SE را اجرا می‌کنند قابلیت اجرای Smart Install را ندارند اما می‌توانند سرویس‌گیرنده این ویژگی باشند اگر از فرمان EXEC مجاز archive download-sw پشتیبانی کنند. برای تعیین فعال بودن ویژگی Smart Install از دستور EXEC مجاز show vstack config استفاده کنید. خروجی این دستور (در صورت فعال بودن این ویژگی) یکی از حالات زیر است: Role: Client and Oper Mode: Enabled Role: Client (SmartInstall enabled) برای تعیین اینکه کدام نسخه Cisco IOS Software بر روی دستگاه اجرا می‌شود ابتدا به دستگاه لاگین کنید سپس از دستور show version در CLI استفاده کنید. اگر نرم‌افزار بر روی دستگاه در حال اجرا باشد در قسمت system banner متنCisco Internetwork Operating System Software یا Cisco IOS Software نشان داده می‌شود. در ادامه نام نرم افزار نسخه آن نیز نمایش داده شده است. برای نرم‌افزار IOS XE نیز به همین صورت است. در زیر دو نمونه خروجی دستور show version نشان داده

	شده‌است. Router> **show version** Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2015 by Cisco Systems, Inc. Compiled Mon 22-Jun-15 09:32 by prod_rel_team --- ios-xe-device# **show version** Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2016 by Cisco Systems, Inc. Compiled Sun 27-Mar-16 21:47 by mcpre
راه حل	سیسکو به‌روزرسانی‌های این نرم‌افزار را که به این آسیب‌پذیری اشاره دارد به صورت رایگان منتشر کرده‌است. کاربران فقط می‌توانند نرم‌افزاری را که قبلا خریداری کرده‌اند و لایسنس معتبر آن را دارند دانلود کنند.

بحرانی (Critical)	Cisco Digital Network Architecture Center Unauthorized Access Vulnerability
عنوان	آسیب‌پذیری دسترسی غیرمجاز در Cisco Digital Network Architecture Center
شناسه آسیب‌پذیری	CVE-2018-0268
CVSS Score	Base – 10.0
نسخه	1.0 Final
شناسه باگ‌های سیسکو	CSCvi47253
تاثیر	دسترسی غیرمجاز (Unauthorized Access)

تاریخ به‌روزرسانی	2018 May 16 16:00 GMT
توضیحات	این آسیب‌پذیری در زیر سیستم مدیریتی کانتینر (container) در مرکز Cisco Digital Network Architecture (DNA) می‌تواند امکان دور زدن احراز هویت و به دست آوردن سطح دسترسی بالاتر را برای مهاجم از راه دور فراهم کند. این آسیب‌پذیری ناشی از پیکربندی پیش‌فرض ناامن زیرسیستم مدیریتی کانتینر Kubernetes در مرکز DNA است. مهاجمی که قابلیت دسترسی به پورت سرویس Kubernetes را داشته باشد می‌تواند دستوراتی با سطح دسترسی بالاتر اجرا کند. سیسکو به روز رسانی های نرم افزاری را که مربوط به این آسیب پذیری است منتشر کرده است.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر نرم‌افزار Cisco DNA Center نسخه 1.1.3 و نسخه‌های قبل از آن تاثیرگذار است. برای مشخص کردن نسخه نرم‌افزار DNA Center می‌توانید با استفاده از مرورگر وب و از طریق پروتکل HTTPS به Cisco DNA Center GUI لاگین کنید. بر روی setting کلیک کرده و گزینه About DNA Center را از منوی کشویی انتخاب کنید. بر روی Show Packages کلیککنید تا نسخه نرم‌افزار را ببینید.
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

بحرانی (Critical)	Cisco Digital Network Architecture Center Authentication Bypass Vulnerability
عنوان	آسیب‌پذیری دسترسی غیرمجاز در Cisco Digital Network Architecture Center
شناسه آسیب‌پذیری	CVE-2018-0271
CVSS Score	Base – 10.0
نسخه	1.0 Final
شناسه باگ‌های سیسکو	CSCvi09394
تاثیر	Authentication Bypass(دور زدن احراز هویت)
تاریخ به‌روزرسانی	2018 May 16 16:00 GMT
توضیحات	این آسیب‌پذیری در درگاه‌های API سیسکو Cisco Digital Network Architecture (DNA) می‌تواند به یک مهاجم اجازه دهد تا از راه دور احراز هویت دستگاه را دور زده و به سرویس‌های حیاتی دسترسی داشته باشد. این آسیب‌پذیری ناشی از عدم موفقیت نرمال‌سازی URL ها قبل از درخواست سرویس است. یک مهاجم می‌تواند از طریق یک URL ساختگی از این مشکل سواستفاده کند و دسترسی غیرمجاز به سرویس‌های حیاتی در DNA Center داشته‌باشد.
محصولات آسیب‌پذیر	نسخه‌های 1.1.2 نرم‌افزار Cisco DNA Center و قبل از آن تحت تاثیر این آسیب‌پذیری هستند. برای مشخص کردن نسخه نرم‌افزار DNA Center می‌توانید با استفاده از مرورگر وب و از طریق پروتکل HTTPS به Cisco DNA Center GUI لاگین کنید. بر روی setting کلیک کرده و گزینه About DNA Center را از منوی کشویی انتخاب کنید. بر روی Show Packages کلیک کنید تا نسخه نرم‌افزار را ببینید.
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه را دانلود نمایید.

بحرانی (Critical)	Cisco Digital Network Architecture Center Static Credentials Vulnerability
عنوان	آسیب‌پذیری Static Credentials در Cisco Digital Network Architecture Center
شناسه آسیب‌پذیری	CVE-2018-0222
CVSS Score	Base – 10.0
نسخه	1.0 Final
شناسه باگ‌های سیسکو	CSCvh98929
تاثیر	اعتبارات ایستا (Static Credentials)
تاریخ به‌روزرسانی	2018 May 16 16:00 GMT
توضیحات	این آسیب‌پذیری در مرکز Cisco Digital Network Architecture (DNA) می‌تواند به یک مهاجم اجازه دهد با یک حساب administrative پیش‌فرض از راه دور به یک سیستم آسیب‌پذیر بدون احراز هویت لاگین کند. این آسیب‌پذیری ناشی از عدم ثبت اعتبارات کاربر ایستا برای یک حساب administrative پیش‌فرض در نرم‌افزار آسیب‌دیده است. مهاجم می‌تواند با استفاده از این حساب به سیستم آسیب‌دیده لاگین کند و دستورات دلخواه خود را با سطح دسترسی root اجرا کند.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر نرم‌افزار Cisco DNA Center نسخه 1.1.3 و نسخه‌های قبل از آن تاثیرگذار است. برای مشخص کردن نسخه نرم‌افزار DNA Center می‌توانید با استفاده از مرورگر وب و از طریق پروتکل HTTPS به Cisco DNA Center GUI لاگین کنید. بر روی setting کلیک کرده و گزینه About DNA Center را از منوی کشویی انتخاب کنید. بر روی Show Packages کلیک کنید تا نسخه نرم‌افزار را ببینید.
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه را دانلود نمایید.

بحرانی (Critical)	Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability
عنوان	آسیب‌پذیری اجرای کد از راه دور و منع سرویس در Cisco Adaptive Security Appliance
شناسه آسیب‌پذیری	CVE-2018-0101
CVSS Score	Base – 10.0
نسخه	2.4 Final
شناسه باگ‌های سیسکو	CSCvg35618 CSCvh79732 CSCvh81737 CSCvh81870
تاثیر	آسیب‌پذیری اجرای کد از راه دور(Remote Code Execution) و منع سرویس(Denial of Service)
تاریخ به‌روزرسانی	2018 May 17 17:52 GMT
توضیحات	این آسیب‌پذیری در ۵ فوریه ۲۰۱۸ به‌روزرسانی شده بود. اما اکنون سیسکو ویژگی‌ها و بردارهای حمله بیشتری از این آسیب‌پذیری شناسایی کرده‌است. علاوه براین اصلاحیه قبلی ناقص بوده و در این اصلاحیه نسخه جدید و کامل‌تری ارائه شده‌است. این آسیب‌پذیری در تجزیه‌کننده XML یا XML Parser از نرم‌افزار Adaptive Security Appliance (ASA) سیسکو می‌تواند این مجوز را به مهاجم دهد تا بدون اعتبارسنجی و از راه دور سیستم آسیب‌پذیر را دوباره راه‌اندازی کند یا از راه دورکدی اجرا کند. همچنین می‌تواند پردازش درخواست‌های اعتبارسنجی ورودی VPN را متوقف کند. این آسیب‌پذیری ناشی از موضوعی است که با اختصاص دادن و آزادسازی حافظه در زمان پردازش یک مخرب XML payload است. یک مهاجم می‌تواند با ارسال یک بسته XML ساختگی به اینترفیس آسیب‌پذیر از این آسیب‌پذیری سواستفاده کند و کد دلخواهی را اجرا کند و کنترل کامل سیستم را بدست گیرد(مانند راه‌اندازی مجدد دستگاه آسیب‌پذی یا متوقف کردن پردازش درخواست‌های اعتبار سنجی ورودی VPN). اگر در سیستم ASA سرویس‌های Secure Socket Layer (SSL) یا سرویس‌های دسترسی از راه دور IKEv2 VPN بر روی یک اینترفیس فعال باشند این سیستم آسیب‌پذیر خواهد بود. خطر آسیب‌پذیری نیز بستگی به دسترسی مهاجم به اینترفیس دارد.
محصولات آسیب‌پذیر	لیست محصولات آسیب‌پذیر در زیر آورده شده‌است. • 3000 Series Industrial Security Appliance (ISA) • 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
- ASA 1000V Cloud Firewall
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4110 Security Appliance
- Firepower 4120 Security Appliance
- Firepower 4140 Security Appliance
- Firepower 4150 Security Appliance
- Firepower 9300 ASA Security Module
- Firepower Threat Defense Software (FTD)
- FTD Virtual (FTDv)

نرم افزار ASA

در جدول زیر ستون سمت چپ لیست ویژگی‌های Cisco ASA آسیب‌پذیر را نشان می‌دهد و ستون سمت راست پیکربندی آسیب‌پذیر از طریق دستور show running-config در CLI را نشان می‌دهد.

Feature	Vulnerable Configuration
Adaptive Security Device Manager (ASDM)[1]	http server enable <port> http <remote_ip_address> <remote_subnet_mask> <interface_name>
AnyConnect IKEv2 Remote Access (with client services)	crypto ikev2 enable <interface_name> client-services port <port #> webvpn anyconnect enable
AnyConnect IKEv2 Remote Access (without client services)	crypto ikev2 enable <interface_name> webvpn anyconnect enable
AnyConnect SSL VPN	webvpn enable <interface_name>
Cisco Security Manager[2]	http server enable <port> http <remote_ip_address> <remote_subnet_mask> <interface_name>
Clientless SSL VPN	webvpn enable <interface_name>
Cut-Through Proxy (Not vulnerable unless used in conjunction with other	aaa authentication listener <interface_name> port <number>

vulnerable features on the same port)	
Local Certificate Authority (CA)	crypto ca server no shutdown
Mobile Device Manager (MDM) Proxy[3]	mdm-proxy enable <interface_name>
Mobile User Security (MUS)	webvpn mus password <password> mus server enable port <port #> mus <address> <mask> <interface_name>
Proxy Bypass	webvpn proxy-bypass
REST API[4]	rest-api image disk0:/<image name> rest-api agent
Security Assertion Markup Language (SAML) Single Sign-On (SSO)[5]	N/A

۱ ASDM تنها از یک آی‌پی در رنج فرمان http پیکربندی شده آسیب‌پذیر است.

۲ Cisco Security Manager تنها از یک آی‌پی در رنج فرمان http پیکربندی شده آسیب‌پذیر است.

۳ MDM Proxy ابتدا در نسخه 9.3.1 پشتیبانی شد.

۴ REST API ابتدا در نسخه 9.3.2 پشتیبانی شد. REST API تنها از یک آی‌پی در رنج فرمان http پیکربندی شده آسیب‌پذیر است.

۵ SAML SSO ابتدا در نسخه 9.6 پشتیبانی شد.

با استفاده از دستور show asp table socket | include SSL|DTLS می‌توان SSL یا سوکت آماده دریافت DTLS بر روی هر پورتی را جست‌وجو کند. اگر پیکربندی ASA شامل ویژگی‌های موجود در جدول بالا باشد آسیب‌پذیر است. یک نمونه خروجی با سوکت SSL و DTLS که در حالت listen قرار دارند در زیر آمده‌است.

```
ciscoasa# show asp table socket | include SSL|DTLS
SSL     00185038 LISTEN    172.16.0.250:443   0.0.0.0:*
SSL     00188638 LISTEN    10.0.0.250:443     0.0.0.0:*
DTLS    0018f7a8 LISTEN    10.0.0.250:443     0.0.0.0:*
```

همچنین می‌توان با استفاده از دستور show asp table socket stats protocol ssl اطلاعات SSL را استخراج کرد. این اطلاعات به ما نشان می‌دهد که چه تعداد پیام دریافت شده و بیشتر از verification است که به معنی آسیب‌پذیر بودن دستگاه ASA است.

```
ciscoasa# show asp table socket stats protocol ssl
NP SSL System Stats:
  Handshake Started:        83
  Handshake Complete:       60
  SSL Open:                  7
  SSL Close:               285
  SSL Server:               84
  SSL Server Verify:         0
  SSL Client:                0
```

همچنین با استفاده از دستور show version در CLI می‌توان نسخه نرم‌افزار ASA روی دستگاه را یافت.

نرم‌افزار FTD:

در جدول زیر ستون سمت چپ لیست ویژگی‌های Cisco FTD آسیب‌پذیر را نشان می‌دهد و ستون سمت راست پیکربندی آسیب‌پذیر از طریق دستور show running-config در CLI را نشان می‌دهد.

Feature	Vulnerable Configuration
HTTP Service enabled[1]	http server enable <port #> http <remote_ip_address> <remote_subnet_mask> <interface_name>
AnyConnect IKEv2 Remote Access (with client services)[2,3]	crypto ikev2 enable <interface_name> client-services port <port #> webvpn anyconnect enable
AnyConnect IKEv2 Remote Access (without client services)[2,3]	crypto ikev2 enable <interface_name> webvpn anyconnect enable
AnyConnect SSL VPN[2,3]	webvpn enable <interface_name>

۱ ویژگی http از طریق Firepower Threat Defense Platform Settings > HTTP بر روی کنسول مدیریتی Firepower (FMC) فعال است.

۲ ویژگی دسترسی از راه دور VPN از طریق Devices > VPN > Remote Access بر روی FCM یا از طریق Device > Remote Access VPN بر روی مدیریت دستگاه Firepower (FDM) فعال است.

۳ ویژگی دسترسی از راه دور VPN ابتدا در نسخه 6.2.2 پشتیبانی شده‌است.

	با استفاده از دستور show asp table socket | include SSL|DTLS می‌توان SSL یا سوکت آماده دریافت DTLS بر روی هر پورتی را جست‌وجو کند. اگر پیکربندی FTD شامل ویژگی‌های موجود در جدول بالا باشد آسیب‌پذیر است. یک نمونه خروجی با سوکت SSL و DTLS که در حالت listen قرار دارند در زیر آمده‌است. firepower# show asp table socket | include SSL|DTLS SSL 01ffb648 LISTEN 1.1.1.1:443 0.0.0.0:* DTLS 00009438 LISTEN 1.1.1.1:443 0.0.0.0:* همچنین می‌توان با استفاده از دستور show asp table socket stats protocol ssl اطلاعات SSL را استخراج کرد. این اطلاعات به ما نشان می‌دهد که چه تعداد پیام دریافت شده و بیشتر از verification است که به معنی آسیب‌پذیر بودن دستگاه FTD است. firepower# show asp table socket stats protocol ssl NP SSL System Stats: Handshake Started: 44 Handshake Complete: 42 SSL Open: 2 SSL Close: 77 SSL Server: 45 SSL Server Verify: 0 SSL Client: 0 همچنین با استفاده از دستور show version در CLI می‌توان نسخه نرم‌افزار FTD روی دستگاه را یافت.
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه را دانلود نمایید.

Cisco Wireless LAN Controller IP Fragment Reassembly Denial of Service Vulnerability	خطرناک(High)
آسیب‌پذیری منع سرویس در Wireless LAN Controller سیسکو از طریق بارگذاری مجدد IP Fragment	عنوان
CVE-2018-0252	شناسه آسیب‌پذیری
Base - 8.6	CVSS Score
1.0	نسخه
CSCvf89222	شناسه باگ‌های سیسکو
آسیب‌پذیری منع سرویس (DOS)	تاثیر
2018 May 2 16:00 GMT	تاریخ انتشار
یک آسیب‌پذیری در تابع سرهم‌سازی قطعات در IP Version 4 (IPv4) که در نرم افزار کنترل‌کننده شبکه بی‌سیم سیسکو سری‌های ۳۵۰۰ ۵۵۰۰ و ۸۵۰۰ موجود است می‌تواند امکان راه‌اندازی مجدد دستگاه آسیب دیده را برای مهاجم از راه دور فراهم نماید. این عمل می‌تواند موجب حمله منع سرویس گردد. این آسیب‌پذیری زمانی رخ می‌دهد که نرم افزار ذکر شده برخی از بسته های IPV4 را دوباره بارگذاری نماید. مهاجم می‌تواند با ارسال fragmentهای ناقصIPV4 از این آسیب‌پذیری سواستفاده کند. این آسیب‌پذیری در نرم‌افزار Wireless LAN Controllers دو نسخه 8.5.103.0 و 8.5.105.0 وجود دارد. سیسکو به‌روزرسانی‌های نرم‌افزاری را که مربوط به این آسیب‌پذیری است منتشر کرده‌است.	توضیحات
این آسیب‌پذیری بر روی تمام نسخه‌های 8.4 و ماقبل آن برای سری‌های ۵۵۰۰ و ۸۵۰۰ محصول Wireless LAN Controllers و همچنین دو نسخه 8.5.103.0 و 8.5.105.0 برای سری‌های ۳۵۰۰ ۵۵۰۰ و ۸۵۰۰ محصول Wireless LAN Controller تاثیرگذار است. تشخیص نسخه نرم‌افزار Cisco Wireless LAN Controller برای تشخیص اینکه کدام نسخه Cisco Wireless LAN Controller در یک دستگاه اجرا می‌شود می‌توان از رابط وب controller یا CLI استفاده کرد. برای استفاده از رابط وب مراحل زیر را انجام دهید: ۱- با استفاده از مرورگر وارد رابط وب controller شوید. ۲- روی تب Monitor کلیک کنید.	محصولات آسیب‌پذیر

۳- در بخش چپ بر روی Summary کلیلک کنید.

۴- در زیر Controller Summary نسخه نرم‌افزار که در حال حاضر بر روی دستگاه اجرا می‌شود را نشان می‌دهد.

برای استفاده از CLI از طریق Telnet به‌controller لاگین کنید دستور show sysinfo را صادر کرده و سپس در خروجی دستور به مقدار فیلد Product Version مراجعه کنید. مثال زیر نمایشی از خروجی این دستور برای دستگاهی که نرم افزار Cisco WLC نسخه 8.3.102.0 است.

```
(wlc)> show sysinfo

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 8.3.102.0
Bootloader Version..... 1.0.1
Field Recovery Image Version..... 6.0.182.0
Firmware Version..... FPGA 1.3, Env 1.6, USB console 1.27
Build Type..... DATA + WPS
```

برای تعیین اینکه کدام نسخه Cisco Mobility Express Software در یک دستگاه اجرا می شود می‌توان از رابط وب یا CLI دستگاه استفاده کرد. برای استفاده از رابط وب مراحل زیر را انجام دهید:

۱- با استفاده از مرورگر به رابط وب وارد شوید.

۲- گزینه System Software > Software Upgrade را انتخاب کنید.

۳- به مقدار فیلد System Software Version مراجعه کنید.

۴- از طریق Telnet یا نشست SSH به اکسس پوینت لاگین کنید.

۵- دستور show version را صادر کرده و به خروجی آن مراجعه کنید.

مثال زیر نمایشی از خروجی این دستور برای اکسس پوینت Cisco Aironet 1852i که نرم‌افزار Cisco Mobility Express نسخه 8.3.111.0 را اجرا می‌کند است.

```
AP# show version


cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K
bytes of memory.


Processor board ID RFDP2BCR021

AP Running Image : 8.3.111.0

Primary Boot Image : 8.3.111.0
```

	Backup Boot Image : 8.1.106.33 AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

خطرناک(High)	Cisco Meeting Server Remote Code Execution Vulnerability
عنوان	آسیب‌پذیری اجرای کد از راه دور در Cisco Meeting Server
شناسه آسیب‌پذیری	CVE-2018-0262
CVSS Score	Base - 8.8
نسخه	1.0
شناسه باگ‌های سیسکو	CSCvg76469
تاثیر	اجرای کد از راه دور(Remote Code Execution)
تاریخ انتشار	2018 May 2 16:00 GMT
توضیحات	سرور جلسه سیسکو (CMS) قابلیت‌های ویدئویی صوتی و اشتراک‌گذاری محتوا را به نرم افزارهایی می‌دهد که از طریق یک اتاق کنفرانس دسکتاپ یا دستگاه تلفن همراه قابل دسترسی هستند. CMS در اتاق‌های ویدیو سیسکو و از طریق ارتباط اسکایپ معماری meeting یکپارچه‌ای را فراهم می‌کند که این قابلیت از طریق همکاری بین سیسکو و Acano که در اوایل سال ۲۰۱۶ به سیسکو پیوست وجود دارد. یک آسیب پذیری در Cisco Meeting Server می‌تواند به یک مهاجم اجازه دسترسی غیرمجاز به اجزا یا اطلاعات حساس در سیستم آسیب دیده را از راه دور بدهد. آسیب‌پذیری ناشی از پیکربندی پیش‌فرض نادرست دستگاه است که می‌تواند رابط‌های داخلی و پورت‌های رابط خارجی سیستم را افشا کند. این آسیب‌پذیری می‌تواند دسترسی غیرمجاز به فایل‌های پایگاه داده و پیکربندی در یک سیستم آسیب‌پذیر را فراهم کند. علاوه بر این اگر سرویس Traversal Using Relay NAT (TURN) فعال شود و با استفاده از اتصالات Transport Layer Security (TLS) مهاجم می‌تواند از اعتبار TURN برای ارسال ترافیک به daemonهای دستگاه(فرایندهایی در پشت زمینه که به صورت مستمر منتظر پاسخ به درخواست‌ها هستند) استفاده کن و مجوز بهره‌برداری از راه دور را کسب کند.

	سیسکو به روزرسانی‌های نرم افزاری را که مربوط به این آسیب پذیری است منتشر کرده است.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی پلت‌فرم Cisco Meeting Server (CMS) Acano X-series نسخه‌های قبل از 2.2.11 تاثیرگذار است. با استفاده از فرمان version در CLI می‌توان نسخه CMS اجرایی روی یک دستگاه را بدست آورد: system> version 2_2_11 اگر در پیکربندی دستورات turn tls و turn certs نمایش داده شود به این معنی است که TLS برای اجرا با TURN server پیکربندی شده‌است. برای چک کردن پیکربندی Mainboard Management Processor (MMP) TLS برای TURN server ادمین باید از دستور turn در کنسول MMP استفاده کند. در مثال زیر یک سیستم با TLS پیکربندی شده برای TURN server نشان داده شده است. cms > turn Enabled: true Username: cisco Password: 1234 Realm: nicedet.com Public IP: none Relay address: 1.2.3.4 TLS port: 3479 TLS cert: turn.crt TLS key: turn.key TLS bundle: none Listen interface a
راه حل	در بخش Products & Services > Collaboration > Cisco Meeting Server > Download Software > Acano X-series آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

خطرناک(High)	Cisco Aironet 1810, 1830, and 1850 Series Access Points Point-to-Point Tunneling Protocol Denial of Service Vulnerability
عنوان	آسیب‌پذیری منع سرویس در پروتکل Point-to-Point Tunneling در اکسس پوینت‌های سیسکوAironet سری 1850, 1830, 1810
شناسه آسیب‌پذیری	CVE-2018-0234
CVSS Score	Base - 8.6
نسخه	1.0
شناسه باگ‌های سیسکو	CSCvf73890
تاثیر	آسیب‌پذیری منع سرویس (DOS)
تاریخ انتشار	2018 May 2 16:00 GMT
توضیحات	این آسیب‌پذیری در پروتکل Point-to-Point Tunneling Protocol (PPTP) در اکسس پوینت‌های سری ۱۸۱۰ ۱۸۳۰ و ۱۸۵۰ موجود است. این آسیب‌پذیری می‌تواند به یک مهاجم کمک کند تا یک دستگاه آسیب دیده را از راه دور دوباره بارگذاری کند و موجب حملات DOS گردد. این آسیب‌پذیری ناشی از اعتبارسنجی نامناسب در فریم‌های Generic Routing Encapsulation (GRE) است. مهاجم می تواند از یک دستگاه که به عنوان یک اکسس‌پوینت به یک شبکه بی‌سیم مشابه رجیستر شده یک اتصال PPTP به اکسس‌پوینت آسیب‌پذیر ایجاد کند و با ارسال یک فریم GRE مخرب امکان دسترسی به آن دستگاه فراهم گردد. مهاجم با ایجاد یک تصادم در فرایند هسته NSS موجب بارگذاری مجدد اکسس‌پوینت و درنتیجه وضعیت DOS می‌شود. سیسکو به‌روزرسانی‌های نرم‌افزاری را که مربوط به این آسیب‌پذیری است منتشر کرده است.
محصولات آسیب‌پذیر	اکسس‌پوینت‌های Cisco Aironet سری ۱۸۱۰ ۱۸۳۰ و ۱۸۵۰ که نرم‌افزار Cisco Mobility Express نسخه‌های 8.4.100.0 8.5.103.0 یا 8.5.105.0 بر روی آنها در حال اجراست تحت تاثیر این آسیب‌پذیری قرار دارند. برای تعیین اینکه کدام نسخه نرم‌افزار Cisco Mobility Express در حال اجراست می‌توان از رابط‌کاربری وب کنترل کننده یا محیط CLI اکسس پوینت استفاده کرد. برای اطلاع از نسخه نرم‌افزار ذکر شده در رابط‌کاربری وب کنترل کننده مراحل زیر را طی کنید: ۱- در مرورگر خود به رابط‌کاربری وب لاگین کنید. ۲- گزینه Management > Software Update را انتخاب کنید.

	۳- به عددی که در بالای صفحه نشان داده شده رجوع کنید. در محیط CLI اکسس‌پوینت ابتدا از طریق Telnet یا SSH به اکسس‌پوینت لاگین کنید. سپس دستور show version را وارد کنید. در خروجی آن می‌توانید نسخه نرم‌افزار را مشاهده کنید. AP# show version cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory. Processor board ID RFDP2BCR021 AP Running Image : 8.3.111.0 Primary Boot Image : 8.3.111.0 Backup Boot Image : 8.1.106.33 AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

Cisco Aironet 1800, 2800, and 3800 Series Access Points Secure Shell Privilege Escalation Vulnerability	**خطرناک(High)**
آسیب‌پذیری ارتقای سطح دسترسی در اکسس‌پوینت‌های Cisco Aironet سری ۱۸۱۰ ۱۸۳۰ و ۱۸۵۰	**عنوان**
CVE-2018-0226	**شناسه آسیب‌پذیری**
Base - 7.6	**CVSS Score**
1.0	**نسخه**
CSCva68116	**شناسه باگ‌های سیسکو**
آسیب‌پذیری ارتقای سطح دسترسی (Privilege Escalation)	**تاثیر**
2018 May 2 16:00 GMT	**تاریخ انتشار**
این آسیب‌پذیری در تخصیص و مدیریت حساب‌های کاربری پیش فرض برای دستیابی به Secure	**توضیحات**

	Shell (SSH) با Cisco Aironet در سری‌های ۱۸۰۰ ۲۸۰۰ و ۳۸۰۰ اکسس پوینت که نرم افزار Cisco Aironet در آن در حال اجراست موجود است. این آسیب‌پذیری به مهاجم امکان دستیابی به امتیازات بالاتر(مانند سطح مدیریتی) در یک اکسس پوینت آسیب‌پذیر را می‌دهد. سیسکو به روز رسانی های نرم افزاری را که مربوط به این آسیب پذیری است منتشر کرده است.
محصولات آسیب‌پذیر	محصولات تحت تاثیر این آسیب‌پذیری به شرح زیر هستند: • Aironet 1800 Series Access Points that are running Cisco Mobility Express Software Releases 8.2.121.0 through 8.5.105.0 • Aironet 2800 Series Access Points that are running Cisco Mobility Express Software Releases 8.3.102.0 through 8.5.105.0 • Aironet 3800 Series Access Points that are running Cisco Mobility Express Software Releases 8.3.102.0 through 8.5.105.0 برای تعیین اینکه کدام نسخه نرم‌افزار Cisco Mobility Express در حال اجراست می‌توان از رابط‌کاربری وب کنترل کننده یا محیط CLI اکسس پوینت استفاده کرد. برای اطلاع از نسخه نرم‌افزار ذکر شده در رابط‌کاربری وب کنترل کننده مراحل زیر را طی کنید: ۱- در مرورگر خود به رابط‌کاربری وب لاگین کنید. ۲- گزینه Management > Software Update را انتخاب کنید. ۳- به عددی که در بالای صفحه نشان داده شده رجوع کنید. در محیط CLI اکسس‌پوینت ابتدا از طریق Telnet یا SSH به اکسس‌پوینت لاگین کنید. سپس دستور show version را وارد کنید. در خروجی آن می‌توانید نسخه نرم‌افزار را مشاهده کنید. AP# show version cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory. Processor board ID RFDP2BCR021 AP Running Image : 8.3.111.0 Primary Boot Image : 8.3.111.0 Backup Boot Image : 8.1.106.33 AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE .

	ارزیابی حساب‌های کاربری و سطوح دسترسی: برای نمایش حساب کاربری برای یک دسترسی Cisco Mobility Express سرپرست می‌تواند به کنترل کننده Cisco Mobility Express لاگین نموده و سپس دستور show mgmtuser را وارد کند. • اگر حساب کاربری اول در لیست خروجی admin باشد و این حساب مجوز read-write را داشته باشد اکسس‌پوینت آسیب‌پذیر نیست. • اگر حساب کاربری اول در لیست خروجی مجوز read-only را داشته باشد یا حساب کاربری loby admin باشد اکسس‌پوینت آسیب‌پذیر است. مثال زیر خروجی دستور show mgmtuser برای پیکربندی بدون آسیب‌پذیری نشان می‌دهد. (wlc)> show mgmtuser User Name Permissions Description Password Strength Telnet Capable ---------- ---------- ---------- ---------- ---------- admin read-write Strong Yes test read-write Strong Yes
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به محصولات تحت تاثیر این آسیب‌پذیری را دانلود نمایید.

Cisco Aironet 1800, 2800, and 3800 Series Access Points Secure Shell Privilege Escalation Vulnerability	**خطرناک(High)**
آسیب‌پذیری ارتقای سطح دسترسی در اکسس‌پوینت‌های Cisco Aironet سری ۱۸۱۰ ۱۸۳۰ و ۱۸۵۰	**عنوان**
CVE-2018-0226	**شناسه آسیب‌پذیری**
Base - 7.6	**CVSS Score**
1.0	**نسخه**
CSCva68116	**شناسه باگ‌های سیسکو**

تاثیر	آسیب‌پذیری ارتقای سطح دسترسی (Privilege Escalation)
تاریخ انتشار	2018 May 2 16:00 GMT
توضیحات	این آسیب‌پذیری در تخصیص و مدیریت حساب‌های کاربری پیش فرض برای دستیابی به Secure Shell (SSH) با Cisco Aironet در سری‌های ۱۸۰۰ ۲۸۰۰ و ۳۸۰۰ اکسس پوینت که نرم افزار Cisco Aironet در آن در حال اجراپست موجود است. این آسیب‌پذیری به مهاجم امکان دستیابی به امتیازات بالاتر(مانند سطح مدیریتی) در یک اکسس پوینت آسیب‌پذیر را می‌دهد. سیسکو به روز رسانی های نرم افزاری را که مربوط به این آسیب پذیری است منتشر کرده است.
محصولات آسیب‌پذیر	محصولات تحت تاثیر این آسیب‌پذیری به شرح زیر هستند: • Aironet 1800 Series Access Points that are running Cisco Mobility Express Software Releases 8.2.121.0 through 8.5.105.0 • Aironet 2800 Series Access Points that are running Cisco Mobility Express Software Releases 8.3.102.0 through 8.5.105.0 • Aironet 3800 Series Access Points that are running Cisco Mobility Express Software Releases 8.3.102.0 through 8.5.105.0 برای تعیین اینکه کدام نسخه نرم‌افزار Cisco Mobility Express در حال اجراست می‌توان از رابط‌کاربری وب کنترل کننده یا محیط CLI اکسس پوینت استفاده کرد. برای اطلاع از نسخه نرم‌افزار ذکر شده در رابط‌کاربری وب کنترل کننده مراحل زیر را طی کنید: ۴- در مرورگر خود به رابط‌کاربری وب لاگین کنید. ۵- گزینه Management > Software Update را انتخاب کنید. ۶- به عددی که در بالای صفحه نشان داده شده رجوع کنید. در محیط CLI اکسس‌پوینت ابتدا از طریق Telnet یا SSH به اکسس‌پوینت لاگین کنید. سپس دستور show version را وارد کنید. در خروجی آن می‌توانید نسخه نرم‌افزار را مشاهده کنید. AP# show version cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory. Processor board ID RFDP2BCR021 AP Running Image : 8.3.111.0 Primary Boot Image : 8.3.111.0 Backup Boot Image : 8.1.106.33

	AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE . ارزیابی حساب‌های کاربری و سطوح دسترسی: برای نمایش حساب کاربری برای یک دسترسی Cisco Mobility Express سرپرست می‌تواند به کنترل کننده Cisco Mobility Express لاگین نموده و سپس دستور show mgmtuser را وارد کند. • اگر حساب کاربری اول در لیست خروجی admin باشد و این حساب مجوز read-write را داشته باشد اکسس‌پوینت آسیب‌پذیر نیست. • اگر حساب کاربری اول در لیست خروجی مجوز read-only را داشته باشد یا حساب کاربری loby admin باشد اکسس‌پوینت آسیب‌پذیر است. مثال زیر خروجی دستور show mgmtuser برای پیکربندی بدون آسیب‌پذیری نشان می‌دهد. (wlc)> show mgmtuser User Name Permissions Description Password Strength Telnet Capable ---------- ---------- ---------- ---------- ---------- admin read-write Strong Yes test read-write Strong Yes
راه حل	در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به محصولات تحت تاثیر این آسیب‌پذیری را دانلود نمایید.

Cisco IoT Field Network Director Cross-Site Request Forgery Vulnerability	**خطرناک(High)**
آسیب‌پذیری جعل درخواست بین‌سایتی در Cisco IoT Field Network Director	**عنوان**
CVE-2018-0270	**شناسه آسیب‌پذیری**
Base – 8.1	**CVSS Score**
1.0	**نسخه**
CSCvi02448	**شناسه باگ‌های**

سیسکو	
تاثیر	آسیب‌پذیری جعل درخواست بین‌سایتی (Cross-Site Request Forgery (Vulnerability
تاریخ انتشار	2018 May 16 16:00 GMT
توضیحات	این آسیب‌پذیری در اینترفیس مدیریتی تحت وب Cisco IoT Field Network Director (IoT-FND) به یک مهاجم امکان حمله جعل درخواست بین‌سایتی و تغییر داده‌های کاربران و گروه‌های موجود را بر روی دستگاه آسیب‌دیده فراهم می‌کند. این آسیب‌پذیری ناشی از حفاظت ناکافی CSRF در اینترفیس مدیریتی تحت وب بر روی یک یک دستگاه آسیب‌دیده است. یک مهاجم می‌تواند با ترغیب کاربر به دنبال کردن یک لینک مخرب به سواستفاده از این آسیب‌پذیری بپردازد که این عمل می‌تواند منجر به انجام فعالیت‌های دلخواه مهاجم با سطح دسترسی کاربر منجر گردد. در وضعیت خطرناکتر اگر کاربر قربانی دارای سطح دسترسی administrative باشد مهاجم می‌تواند یک حساب کاربری جدید برای کنترل کامل بر روی اینترفیس آسیب‌دیده ایجاد کند.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی محصولات سیسکو زیر تاثیر دارند. • Connected Grid Network Management System, if running a software release prior to IoT-FND Release 3.0. • IoT Field Network Director, if running a software release prior to IoT-FND Release 4.1.1-6 or 4.2.0-123.
راه حل	در بخش Products > Cloud and Systems Management > IoT Management and Automation > IoT Field Network Director در سایت سیکو آپدیت‌های مربوط به محصولات تحت تاثیر این آسیب‌پذیری را دانلود نمایید.

Cisco Identity Services Engine EAP TLS Certificate Denial of Service Vulnerability	**خطرناک(High)**
آسیب‌پذیری منع سرویس در پروتکل اعتبارسنجی گواهی EAP TLS سیسکو	**عنوان**
CVE-2018-0277	**شناسه آسیب‌پذیری**
Base – 8.6	**CVSS Score**
1.0	**نسخه**

شناسه باگ‌های سیسکو	CSCve31857
تاثیر	آسیب‌پذیری منع سرویس (Denial of Service Vulnerability)
تاریخ انتشار	2018 May 16 16:00 GMT
توضیحات	این آسیب‌پذیری در اعتبارسنجی گواهی پروتکل امنیتی لایه انتقال Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) در حین تصدیق EAP برای موتور سرویس‌های احرازهویت سیسکو Identity Services Engine (ISE) وجود دارد. مهاجمی می‌تواند با سواستفاده از این آسیب‌پذیری سرور برنامه کاربردی ISE دوباره راه‌اندازی کند و درنتیجه آن شرایط حمله منع سرویس برای یک دستگاه آسیب‌دیده فراهم شود. این آسیب‌پذیری ناشی از اعتبارسنجی ناقص ورودی گواهی EAP-TLS کلاینت است. یک مهاجم می‌تواند با استفاده از این آسیب‌پذیری سرور برنامه کاربردی ISE را دوباره راه‌اندازی (restart) کند در حالیکه کلاینت در تلاش برای برقراری اتصال تصدیق EAP است. مهاجم برای این حمله نیاز به اعتبار administrator دارد.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی محصولات سیسکو زیر تاثیر دارند. • Cisco ISE • Cisco ISE Express • Cisco ISE Virtual Appliance برای تعیین اینکه کدام نسخه از نرم افزار در حال حاضر در یک دستگاه اجرا می شود باید از دستور show version در محیط CLI دستگاه استفاده کرد. روش دیگر برای تعیین نسخه نرم‌افزار در پورتال ادمین به گوشه سمت راست رفته بر روی setting و سپس About Identity Service Engine کلیک کنید. نمونه خروجی show version دستور در محیط CLI در زیر نشان داده شده‌است. ServiceEngine115/admin# show version Cisco Application Deployment Engine OS Release: 2.3 ADE-OS Build Version: 2.3.0.187 ADE-OS System Architecture: x86_64 Copyright (c) 2005-2014 by Cisco Systems, Inc. All rights reserved. Hostname: ServiceEngine115
راه حل	به‌روزرسانی‌های این نرم‌افزار آسیب‌پذیر را از سایت سیسکو دانلود نمایید.

Cisco Meeting Server Media Services Denial of Service Vulnerability	خطرناک(High)
آسیب‌پذیری منع سرویس در سرویس‌های Meeting Server Media سیسکو	عنوان
CVE-2018-0280	شناسه آسیب‌پذیری
Base – 7.5	CVSS Score
1.0	نسخه
CSCve79693 CSCvf91393 CSCvg64656 CSCvh30725 CSCvi86363	شناسه باگ‌های سیسکو
آسیب‌پذیری منع سرویس (Denial of Service)	تاثیر
2018 May 16 16:00 GMT	تاریخ انتشار
سرور Meeting Server سیسکو قابلیت‌های ویدئویی صوتی و اشتراک‌گذاری محتوا را به نرم افزاری می‌دهد که می‌تواند از طریق اتاق کنفرانس دسکتاپ یا دستگاه تلفن همراه قابل دسترسی باشد. سرورMeeting Server سیسکو در سراسر اتاق‌های ویدیویی سیسکو کار می‌کند و از طریق اسکایپ برای کسب وکار و دیگر ارائه دهندگان سخت‌افزار متصل می‌شود تا نعماری meeting یکپارچه‌ای ایجاد کند. این قابلیت از طریق همکاری بین سیسکو و Acano که توسط سیسکو در سال ۲۰۱۶ به دست آمد وجود دارد. این آسیب‌پذیری در پردازش بیتی پروتکل Real-Time Transport Protocol (RTP) در سرور Meeting Server سیسکو شرایط منع سرویس را برای یک مهاجم می‌تواند فراهم کند. این آسیب‌پذیری ناشی از اعتبارسنجی ناکافی ورودی در رشته بیت‌های(bitstream) پروتکل RTP می‌باشد. مهاجمی می‌تواند با ارسال یک رشته بیت RTP ساختگی به یک سرور Meeting سیسکو آسیب‌پذیر موجب منع خدمات صوتی و ویدیویی به واسطه تخریب فرایند Media و درنتیجه ایجاد شرایط منع سرویس گردد.	توضیحات

محصولات آسیب‌پذیر	محصولات Cisco Meeting Server که نرم‌افزار Cisco Meeting Server نسخه‌های 2.0، 2.1، 2.2 و 2.3 بر روی آنها اجرا می‌شود تحت تاثیر این آسیب‌پذیری قرار دارند. برای تعیین نسخه نرم‌افزار Cisco Meeting Server در محیط CLI فرمان version را صادر کرده تا در خروجی آن نسخه نرم‌افزار را مشاهده کنید. مثال زیر نمونه‌ای از خروجی این دستور است. system> version 2_2_11
راه حل	در نسخه‌های ۲,۱,۱۲ ۲,۲,۱۰ و ۲,۳,۱ این آسیب‌پذیری رفع شده‌اند. جهت دانلود این نسخه‌ها به سایت سیسکو مراجعه کنید.

Cisco Enterprise NFV Infrastructure Software Linux Shell Access Vulnerability	**خطرناک(High)**
آسیب‌پذیری دسترسی به Linux Shell در نرم‌افزار Enterprise NFV	**عنوان**
CVE-2018-0279	**شناسه آسیب‌پذیری**
Base – 6.3	**CVSS Score**
1.0	**نسخه**
CSCvh25026	**شناسه باگ‌های سیسکو**
آسیب‌پذیری دسترسی به Linux Shell	**تاثیر**
2018 May 16 16:00 GMT	**تاریخ انتشار**
این آسیب‌پذیری مربوط به سرور Secure Copy Protocol (SCP) در نرم‌افزار Enterprise NFV سیسکو (NFVIS) امکان دسترسی به shell سیستم‌عامل لینوکس در دستگاه آسیب‌پذیر را برای مهاجم از راه دور فراهم می‌کند. این آسیب‌پذیری ناشی از اعتبارسنجی و تصدیق نامناسب ورودی در آرگومان‌های دستورات می‌باشد. مهاجمی با استفاده از آرگومان‌های ساختگی حین باز کردن یک ارتباط با دستگاه آسیب‌دیده می‌تواند با یک حساب کاربری غیر ریشه (non-root) به shell سیستم‌عامل لینوکس دستگاه آسیب‌دیده دسترسی پیدا کند. با توجه به طراحی سیستم دسترسی به shell لینوکس امکان	**توضیحات**

	اجرای حملات اضافی را فراهم می‌کند که ممکن است تأثیر قابل توجهی در سیستم آسیب‌دیده داشته باشد.
محصولات آسیب‌پذیر	دستگاه‌هایی که نرم‌افزار Enterprise NFV نسخه‌های 3.6.3، 3.7.1 و نسخه‌های قبل از آن بر روی آنها اجرا می‌شود و مجاز به دسترسی به سرور SCP هستند تحت تاثیر این آسیب‌پذیری هستند. نسخه‌های 3.5.x و 3.6.x به صورت پیشفرض اجازه دسترسی به سرور SCP را می‌دهند درحالیکه نسخه 3.7.1 این مجوز را نمی‌هد. برای تعیین نسخه نرم‌افزار NFVIS باید از دستور show version در محیط CLI استفاده کرد. مثال زیر یک نمونه خروجی این دستور است. encs# show version version name "Cisco NFV Infrastructure Software" version version 3.7.1-FC2 نرم‌افزار NFVIS نسخه 3.7.1 مجوز دسترسی به سرور SCP را درصورتی می‌دهد که با وارد کردن دستور system settings ip-receive-acl در CLI خروجی[service [scpd و action accept نمایش داده شود. مثال زیر یک نمونه خروجی از این دستور بر روی دستگاهی است که مجوز دسترسی به سرور SCP را می‌دهد. encs# show running-config | begin ip-receive-acl system settings ip-receive-acl 192.0.2.0/24 service [scpd] action accept توجه: نرم‌افزار NFVIS نسخه‌های 3.6.3، 3.7.1 و نسخه‌های قبل از آن دستور system settings ip-receive-acl در CLI پشتیبانی نمی‌کنند. در این نسخه‌ها همواره مجوز دسترسی به سرور SCP فعال است و قابل غیرفعال‌سازی نیست. توجه: سازمان‌هایی که نسخه‌های 3.5.x و 3.6.x نرم‌افزار NFVIS را اجرا می‌کنند و نیازی به استفاده از سرور SCP ندارند توصیه می‌گردد که از فایروال خارجی برای محدود کردن دسترسی به پورت TCP 22222 بر روی دستگاه آسیب‌دیده استفاده کنند.
راه حل	در بخش software center سایت سیسکو مسیر Downloads Home > Routers > Network Functions Virtualization > Enterprise NFV Infrastructure Software > NFV Infrastructure Software را برای دانلود به‌روزرسانی نرم افزار NFVIS دنبال کنید.

متوسط (Medium)	CPU Side-Channel Information Disclosure Vulnerabilities: May 2018
عنوان	آسیب‌پذیری افشای اطلاعات کانال جانبی(Side-Channel) در CPU
شناسه آسیب‌پذیری	CVE-2018-3639 CVE-2018-3640
CVSS Score	-
نسخه	1.0
شناسه باگ‌های سیسکو	-
تاثیر	-
تاریخ انتشار	2018 May 22 01:00 GMT
توضیحات	در تاریخ ۲۱ می ۲۰۱۸ محققان دو آسیب‌پذیری را کشف کردند که با بهره گیری از اجرای کد در بسیاری از معماری میکروپروسسورهای مدرن به انجام حملات افشای اطلاعات می‌پردازد. مهاجم محلی (بدون امتیاز) با بهره‌گیری از این آسیب‌پذیری می‌تواند در شرایط خاص بخشی از حافظه که اجازه دسترسی به آن‌را ندارد و متعلق به فرایندی دیگر است را بخواند. آسیب‌پذیری CVE-2018-3639 به عنوان Spectre Variant 4 یا SpectreNG و همچنین آسیب‌پذیری دوم CVE-2018-3640 به عنوان Spectre Variant 3a شناخته شده‌اند. هر دوی این حملات در ژانویه ۲۰۱۸ کشف شدند و حملات cache-timing را برای دستیابی به هر داده فاش شده انجام می‌دهند. برای بهره‌برداری از هر یک از این آسیب‌پذیری‌ها مهاجم باید قادر به اجرای کد ایجاد شده یا اسکریپتی در دستگاه آسیب دیده باشد. گرچه ترکیب CPU و سیستم‌عامل در یک دستگاه یا سرویس ممکن است تحت تاثیر این اسیب‌پذیری قرار گیرد؛ اکثر محصولات سیسکو سیستم‌های بسته ای هستند و که به کاربران اجازه اجرای کدی را نمی‌دهند و بنابراین آسیب‌پذیر نیستند. محصولات سیکو تنها زمانی آسیب‌پذیر هستند اگر به کاربران مجوز اجرای کد خود را در کنار کدهای سیسکو در یک میکروپروسسور داده باشند. یک محصول سیسکو که ممکن است به عنوان یک ماشین مجازی یا کانتینر قرار داده شود حتی اگر مستقیما تحت تاثیر این آسیب‌پذیری‌ها نباشند در صورتیکه محیط میزبان آسیب‌پذیر باشد ممکن است هدف این حملات قرار گیرد. توصیه سیسکو به کاربران خود این است که محیط‌های مجازی خود را مقاوم کنند کنترل سطح دسترسی کاربر را بیشتر نموده و از نصب بروزرسانی‌های جدید امنیتی اطمینان حاصل کنند. همچنین کسانی که محصولات سیسکو را به عنوان دستگاه مجازی در محیط میزبان چند اجاره‌ای در اختیار دارند باید از سخت‌افزار پایه آن برای آسیب‌پذیری‌های ذکر

شده وصله شده‌اند. همچنین سرویس‌های ابری Cisco به طور مستقیم تحت تاثیر این آسیب‌پذیری‌ها قرار نمی‌گیرند اما باید توجه داشت که زیرساخت‌های مورد استفاده آنها ممکن است تحت تاثیر قرار گیرد. در بخش بعدی محصولاتی که عدم تاثیرپذیری آنها به این دو آسیب‌پذیری تایید شده است آورده شده است. با توجه به ادامه روند تحقیقات سیسکو توصیه می‌گردد به صورت مرتب اطلاعیه‌های شرکت سیسکو در رابطه با محصولات تحت تاثیر را دنبال نمایید.

محصولات آسیب‌پذیر

سیسکو در حال بررسی خط تولید خود برای تعیین اینکه کدام محصولات و سرویس‌های ابری ممکن است تحت تاثیر این آسیب‌پذیری باشند است. با پیشرفت تحقیقات سیسکو اطلاع‌رسانی خود را با اطلاعاتی در مورد محصولات و خدمات تحت تاثیر شناسه باگ سیسکو برای هر محصول یا خدمات آسیب دیده را به‌روزرسانی خواهد کرد.

شرکت سیسکو بعد از بررسی لیستی از محصولات آسیب‌پذیر خود را به صورت جدول زیر معرفی کرده است.

Product	Cisco Bug ID	Fixed Release Availability
Network Management and Provisioning		
Cisco Network Functions Virtualization Infrastructure Software	CSCvj59161	
Routing and Switching - Enterprise and Service Provider		
Cisco 800 Series Industrial Integrated Services Routers	CSCvj59153	
Cisco ASR 9000 XR 64-bit Series Routers	CSCvj59142	
Cisco CGR 1000 Compute Module (IOx feature)	CSCvj59160	
Cisco NCS 1000 Series Routers	CSCvj59142	
Cisco NCS 5000 Series Routers	CSCvj59142	
Cisco NCS 5500 Series Routers	CSCvj59142	
Cisco XRv 9000 Series Routers	CSCvj59142	
Unified Computing		
Cisco UCS B-Series M2 Blade Servers	CSCvj59301	

Cisco UCS B-Series M3 Blade Servers	CSCvj54880	Cisco UCS B-Series M3 Blade Servers (Estimated Late June 2018) Cisco UCS C-Series M3 Rack Servers (Estimated Late June 2018)
Cisco UCS B-Series M4 Blade Servers (except B260, B460)	CSCvj54187	Cisco UCS B-Series M4 Blade Servers (except B260 B460) (Estimated Late June 2018) Cisco UCS C-Series M4 Rack Servers (except C460) (ETA Late June 2018) Cisco UCS S3260 M4 Storage Server (Estimated Late June 2018)
Cisco UCS B-Series M5 Blade Servers	CSCvj59266	Cisco UCS B-Series M5 Blade Servers (Estimated Late June 2018) Cisco UCS C-Series M5 Rack Servers (Estimated Late June 2018)
Cisco UCS B260 M4 Blade Server	CSCvj54847	Cisco UCS B260 M4 Blade Server (Estimated Late June 2018) Cisco UCS B460 M4 Blade Server (Estimated Late June 2018) Cisco UCS C460 M4 Rack Server (Estimated Late June 2018)
Cisco UCS B460 M4 Blade Server	CSCvj54847	Cisco UCS B260 M4 Blade Server (Estimated Late June 2018) Cisco UCS B460 M4 Blade Server (Estimated Late June 2018) Cisco UCS C460 M4 Rack Server (Estimated Late June 2018)
Cisco UCS C-Series M2 Rack Servers	CSCvj59301	
Cisco UCS C-Series M3 Rack Servers	CSCvj54880	Cisco UCS B-Series M3 Blade Servers (Estimated Late June 2018) Cisco UCS C-Series M3 Rack Servers (Estimated Late June 2018)
Cisco UCS C-Series M4 Rack Servers (except C460) [1]	CSCvj54187	Cisco UCS B-Series M4 Blade Servers (except B260 B460) (Estimated Late June 2018) Cisco UCS C-Series M4 Rack Servers (except C460) (Estimated

		Late June 2018) Cisco UCS S3260 M4 Storage Server (Estimated Late June 2018)	
Cisco UCS C-Series M5 Rack Servers [1]	CSCvj59266	Cisco UCS B-Series M5 Blade Servers (Estimated Late June 2018) Cisco UCS C-Series M5 Rack Servers (Estimated Late June 2018)	
Cisco UCS C460 M4 Rack Server	CSCvj54847	Cisco UCS B260 M4 Blade Server (Estimated Late June 2018) Cisco UCS B460 M4 Blade Server (Estimated Late June 2018) Cisco UCS C460 M4 Rack Server (Estimated Late June 2018)	
Cisco UCS S3260 M4 Storage Server	CSCvj54187	Cisco UCS B-Series M4 Blade Servers (except B260 B460) (Estimated Late June 2018) Cisco UCS C-Series M4 Rack Servers (except C460) (Estimated Late June 2018) Cisco UCS S3260 M4 Storage Server (Estimated Late June 2018)	
-			**راه حل**

در ادامه لیستی از آسیب‌پذیری‌های با درجه حساسیت متوسط که شرکت سیسکو در ماه می منتشر کرده‌است نشان داده شده‌است.

شناسه آسیب‌پذیری	عنوان آسیب‌پذیری
CVE-2018-0247	Cisco Wireless LAN Controller and Aironet Access Points IOS WebAuth Client Authentication Bypass Vulnerability
CVE-2018-0250	Cisco Aironet Access Points Central Web Authentication FlexConnect Client ACL Bypass Vulnerability
CVE-2018-0283	**Cisco Firepower System Software Transport Layer Security Denial of Service Vulnerability**
CVE-2018-0278	**Cisco Firepower System Software Cross-Origin Domain Protection Vulnerability**

CVE-2018-0281	Cisco Firepower System Software Transport Layer Security Extensions Denial of Service Vulnerability
CVE-2018-0286	**Cisco IOS XR Software netconf Denial of Service Vulnerability**
CVE-2018-0285	**Cisco Prime Service Catalog User Interface Denial of Service Vulnerability**
CVE-2018-0287	**Cisco WebEx Advanced Recording Format Player Remote Code Execution Vulnerability**
CVE-2018-0245	**Cisco 5500 and 8500 Series Wireless LAN Controller Information Disclosure Vulnerability**
CVE-2018-0249	**Cisco Aironet 1800 Series Access Point 802.11 Denial of Service Vulnerability**
CVE-2018-0288	**Cisco WebEx Recording Format Player Information Disclosure Vulnerability**
CVE-2018-0297	**Cisco Firepower Threat Defense Software Policy Bypass Vulnerability**
CVE-2018-0325	**Cisco IP Phone 7800 Series and 8800 Series Denial of Service Vulnerability**
CVE-2018-0289	**Cisco Identity Services Engine Logs Cross-Site Scripting Vulnerability**
CVE-2018-0290	Cisco SocialMiner Notification System Denial of Service Vulnerability
CVE-2018-0326	**Cisco TelePresence Server Cross-Frame Scripting Vulnerability**
CVE-2018-0324	**Cisco Enterprise NFV Infrastructure Software CLI Command Injection Vulnerability**
CVE-2018-0323	**Cisco Enterprise NFV Infrastructure Software Web Management Interface Path Traversal Vulnerability**
CVE-2018-0327	**Cisco Identity Services Engine Cross-Site Scripting Vulnerability**
CVE-2018-0328	**Cisco Unified Communications Manager and Cisco Unified Presence Cross-Site Scripting Vulnerability**
CVE-2017-12373 CVE-2017-15533 CVE-2017-17428	**Bleichenbacher Attack on TLS Affecting Cisco Products: December 2017**

CWE-200	
CVE-2018-3639 CVE-2018-3640	**CPU Side-Channel Information Disclosure Vulnerabilities: May 2018**
CVE-2018-0326	**Cisco TelePresence TX9000 Series Cross-Frame Scripting Vulnerability**

مراجع

https://tools.cisco.com/security/center/publicationListing.x