مرکزماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش امنیتی محصولات سیسکو با درجه حساسیت Critical در ماه جولای ۲۰۲۰

شرکت Cisco یکی از بزرگترین تولیدکنندگان تجهیزات نرم‌افزاری و سخت‌افزاری شبکه می‌باشد که با توجه به پیشرفت روزافزون 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 و رفع این آسیب‌پذیری‌ها می‌شوند. در این گزارش آسیب‌پذیری‌های با سطح (Critical) ارائه شده است. همچنین محصولاتی که دارای این آسیب‌پذیری‌ها هستند نیز مشخص شده است و با مراجعه به لینک مشخص شده اطلاعات جامع در مورد آسیب‌پذیری و نحوه رفع آن داده شده است.

بحرانی(Critical)	Multiple Vulnerabilities in Treck IP Stack Affecting Cisco Products: June 2020
عنوان	آسیب‌پذیری‌های متعدد در Treck IP Stack تاثیر گذار بر محصولات Cisco: ژوئن ۲۰۲۰
شناسه آسیب‌پذیری	CVE-2020-11896 CVE-2020-11897 CVE-2020-11898 CVE-2020-11899 CVE-2020-11900 CVE-2020-11901 CVE-2020-11902 CVE-2020-11903 CVE-2020-11904 CVE-2020-11905 CVE-2020-11906 CVE-2020-11907 CVE-2020-11908 CVE-2020-11909 CVE-2020-11910 CVE-2020-11911 CVE-2020-11912 CVE-2020-11913 CVE-2020-11914 CWE-20
CVSS Score	Base – 9.8
نسخه	1.4
شناسه باگ‌های	CSCvu60310 CSCvu60313

سیسکو	CSCvu60314
تاثیر	Remote Code Execution Denial Of Service Information Disclosure
تاریخ آخرین به‌روزرسانی	2020 July 17 15:59 GMT
توضیحات	مجموعه‌ای از آسیب‌پذیری‌های ناشناخته در مورد اجرای Track IP stack در تاریخ ۱۶ژوئن سال ۲۰۲۰ گزارش شده‌اند. این آسیب‌پذیری‌ها به‌صورت مشترک با نام Ripple20 شناخته می‌شوند. استفاده از این آسیب‌پذیری‌ها توسط مهاجم میتواند منجر به حملات Dos ، اجرای کد از راه دور، یا افشای اطلاعات شود.
محصولات آسیب‌پذیر	Cisco ASR 5000 Series Routers 21.5.27 (31-Jul-2020) Cisco ASR 5500 21.20.2 (31-Jul-2020) 21.14.22 (31-Jul-2020) 21.5.27 (31-Jul-2020) 21.11.15 (31-Jul-2020) Cisco Virtual Packet Core 21.11.15 (31-Jul-2020) 21.20.2 (31-Jul-2020) 21.14.22 (31-Jul-2020) 21.5.27 (31-Jul-2020)
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC

عنوان	آسیب‌پذیری اعتبار پیش‌فرض استاتیک در Small Business RV110W Wireless-N VPN Firewall سیسکو
شناسه آسیب‌پذیری	CVE-2020-3198 CVE-2020-3258 CWE-119
CVSS Score	Base – 9.8

نسخه	Final1.0
شناسه باگ‌های سیسکو	CSCvs50818
تاثیر	unauthenticated
تاریخ آخرین به‌روزرسانی	2020 July 15 16:00 GMT
توضیحات	آسیب‌پذیری در سرویس Telnet Cisco Small Business RV110W Wireless-N VPN فایروال روتر می‌تواند به یک مهاجم غیرمجاز و از راه دور اجازه دهد تا کنترل کامل دستگاه را با یک حساب ممتاز داشته باشد. این آسیب‌پذیری به دلیل وجود یک حساب کاربری با رمز عبور پیش فرض و استاتیک است. یک مهاجم می‌تواند با استفاده از این حساب پیش فرض برای اتصال به سیستم آسیب دیده از این آسیب‌پذیری استفاده کند. یک بهره برداری موفق می‌تواند به مهاجم اجازه دهد کنترل کامل یک دستگاه آسیب دیده را به دست آورد.
محصولات آسیب‌پذیر	Cisco Small Business RV110W Wireless-N VPN Firewall firmware releases earlier than Release 1.2.2.8.
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv110w-static-cred-BMTWBWTy

بحرانی(Critical)	**Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface Remote Command Execution Vulnerability**
عنوان	آسیب‌پذیری اجرای دستور از راه دور در رابط مدیریت روتر Small Business RV110W, RV130, RV130W, RV215W سیسکو
شناسه آسیب‌پذیری	CVE-2020-3323 CWE-119
CVSS Score	Base 9.8
نسخه	Final 1.0
شناسه باگ‌های	CSCvr97864 CSCvr97884

سیسکو	CSCvr97889
تاثیر	unauthenticated
تاریخ آخرین به‌روزرسانی	2020 July 15 16:00 GMT
توضیحات	آسیب‌پذیری در رابط مدیریت مبتنی بر وب دستگاه‌های کسب‌وکار کوچک سیسکو RV110W ،RV130،RV130W و RV215W می‌تواند به یک مهاجم غیرمجاز و از راه دور اجازه دهد تا کد دلخواه را بر روی یک دستگاه آسیب دیده اجرا کند. این آسیب‌پذیری به دلیل تایید اعتبار نادرست ورودی کاربر در رابط مدیریت مبتنی بر وب است. یک مهاجم می‌تواند با ارسال درخواست‌هایHTTP دستکاری شده به یک دستگاه هدفمند، از این آسیب‌پذیری استفاده کند. یک استفاده موفق می‌تواند به مهاجم اجازه دهد کدهای دلخواه را به عنوان کاربر اصلی در سیستم عامل اصلی دستگاه آسیب دیده اجرا کند.
محصولات آسیب‌پذیر	RV110W Wireless-N VPN Firewall RV130 VPN Router RV130W Wireless-N Multifunction VPN Router RV215W Wireless-N VPN Router
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-AQKREqp

بحرانی(Critical)	Cisco RV110W, RV130, RV130W, and RV215W Routers Authentication Bypass Vulnerability
عنوان	آسیب‌پذیری دور زدن احرازهویت روترهای RV110W, RV130, RV130W,RV215W سیسکو
شناسه آسیب‌پذیری	CVE-2020-3144 CWE-284
CVSS Score	Base 9.8
نسخه	Final 1.0
شناسه باگ‌های سیسکو	CSCvr96247 CSCvr96252 CSCvr96256

تاثیر	Authentication Bypass
تاریخ آخرین به‌روزرسانی	2020 July 15 16:00 GMT
توضیحات	آسیب‌پذیری در رابط مدیریت مبتنی بر وب در فایروال Cisco RV110W Wireless-N VPN، RV130 روتر، Wireless-N VPN RV130W Multifunction VPN ، RV215W Wireless-N VPN می‌تواند به یک مهاجم غیرمجاز، از راه دور با دور زدن احراز هویت دستورات دلخواه با سطح دسترسی اداری در دستگاه آسیب دیده اجرا کند. این آسیب‌پذیری ناشی از مدیریت نادرست جلسه در دستگاه‌های آسیب دیده است. یک مهاجم می‌تواند با ارسال درخواست HTTP دستکاری شده به دستگاه آسیب دیده، از این آسیب‌پذیری استفاده کند. یک بهره‌برداری موفق می‌تواند به مهاجم اجازه دهد تا از طریق دستگاه آسیب دیده دسترسی اداری داشته باشد.
محصولات آسیب‌پذیر	RV110W Wireless-N VPN Firewall RV130 VPN Router RV130W Wireless-N Multifunction VPN Router RV215W Wireless-N VPN Router
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-auth-bypass-cGv9EruZ

بحرانی(Critical)	Cisco RV110W and RV215W Series Routers Arbitrary Code Execution Vulnerability
عنوان	آسیب‌پذیری اجرای کد دلخواه در روترهای سری RV215W و RV110W سیسکو
شناسه آسیب‌پذیری	CVE-2020-3331 CWE-119
CVSS Score	Base 9.8
نسخه	Final1.0
شناسه باگ‌های سیسکو	CSCvs50861 CSCvs50862
تاثیر	Arbitrary Code Execution

تاریخ آخرین به‌روزرسانی	2020 July 15 16:00 GMT
توضیحات	آسیب‌پذیری در رابط مدیریت مبتنی بر وب در فایروال Cisco RV110W Wireless-N VPN و Cisco RV215W Wireless-N VPN می‌تواند به یک مهاجم از راه دور غیرمجاز اجازه دهد تا کد دلخواه را بر روی یک دستگاه آسیب دیده اجرا کند.
محصولات آسیب‌پذیر	RV110W Wireless-N VPN Firewall releases earlier than Release 1.2.2.8 RV215W Wireless-N VPN Router releases earlier than Release 1.3.1.7
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-code-exec-wH3BNFb

بحرانی (Critical)	Cisco Prime License Manager Privilege Escalation Vulnerability
عنوان	آسیب‌پذیری پیمایش امتیاز مجوز اولیه مدیر سیسکو
شناسه آسیب‌پذیری	CVE-2020-3140 CWE-255
CVSS Score	Base 9.8
نسخه	Final1.0
شناسه باگ‌های سیسکو	CSCvq97227
تاثیر	unauthenticated
تاریخ آخرین به‌روزرسانی	2020 July 15 16:00 GMT
توضیحات	آسیب‌پذیری موجود در رابط مدیریت وب نرم افزار Cisco Prime License Manager (PLM) می‌تواند به یک مهاجم غیر مجاز و از راه دور اجازه دهد دسترسی غیرمجاز به یک دستگاه آسیب دیده را بدست آورد.
محصولات آسیب‌پذیر	Cisco PLM Software 10.5(2)SU9 and earlier 11.5(1)SU6 and earlier

راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-prime-priv-esc-HyhwdzBA

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