بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

گزارش امنیتی محصولات سیسکو با درجه حساسیت بحرانی در ماه ژوئن ۲۰۲۰

اخبار بروزرسانی

شناسه سند ..... Maher_1399042

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۴/۱

طبقه‌بندی سند ..... عادی

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

۴۲۶۵۰۰۰۰
(۰۲۱)

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ مقدمه

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 می¬نمایند. در این گزارش آسیب‌پذیری‌های با سطح بحرانی به همراه محصولاتی که دارای این آسیب‌پذیری‌ها هستند و نیز اطلاعات جامع در مورد آسیب‌پذیری و نحوه رفع آن ارائه شده است.

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

۲ آسیب‌پذیری‌های سیسکو با درجه حساسیت بحرانی

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	Interim1.0
شناسه باگ‌های سیسکو	CSCvu60310 CSCvu60313 CSCvu60314
تاثیر	Remote Code Execution Denial Of Service Information Disclosure
تاریخ آخرین به‌روزرسانی	2020 June 17 20:00 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 که اکثر آن‌ها به دلیل نقص‌های موجود در مدیریت حافظه می‌باشند. سوءاستفاده از این آسیب‌پذیری‌ها توسط مهاجم می‌تواند منجر به حملات Dos، اجرای کد از راه دور و یا افشای اطلاعات شود.
محصولات آسیب‌پذیر	Cisco GGSN Gateway GPRS Support Node Cisco MME Mobility Management Entity Cisco PGW Packet Data Network Gateway

	Cisco System Architecture Evolution Gateway (SAEGW)
محصولات در حال بررسی	Cisco ASR 5000 Series Routers Cisco Home Node-B Gateway Cisco IP Services Gateway (IPSG) Cisco PDSN/HA Packet Data Serving Node and Home Agent
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC

بحرانی(Critical)	**Cisco IOS Software for Cisco Industrial Routers Arbitrary Code Execution Vulnerabilities**
عنوان	آسیب‌پذیری اجرا کد دلخواه در نرم‌افزار Cisco IOS برای روترهای صنعتی Cisco
شناسه آسیب‌پذیری	CVE-2020-3198 CVE-2020-3258 CWE-119
CVSS Score	Base – 9.8
نسخه	Final1.0
شناسه باگ‌های سیسکو	CSCvr12083 CSCvr46885
تاثیر	Arbitrary Code Execution
تاریخ آخرین به‌روزرسانی	2020 June 3 16:00 GMT
توضیحات	این آسیب‌پذیری در محصولات زیر می‌تواند به یک مهاجم، از راه دور یا محلی اجازه دهد تا کد دلخواه را بر روی یک سیستم آسیب‌دیده اجرا کند و یا باعث بارگذاری مجدد سیستم آسیب‌دیده شود.
محصولات آسیب‌پذیر	Cisco 809 and 829 Industrial ISRs CGR1000
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH

بحرانی(Critical)	Cisco IOS Software for Cisco Industrial Routers Virtual Device Server Inter-VM Channel Command Injection Vulnerability
عنوان	آسیب‌پذیری تزریق دستور نرم افزار Cisco IOS برای روترهای صنعتی سیسکو Virtual Device Server Inter-VM Channel
شناسه آسیب‌پذیری	CVE-2020-3205 CWE-20
CVSS Score	Base – 8.8
نسخه	Final1.0
شناسه باگ‌های سیسکو	CSCvq66443
تاثیر	Command Injection
تاریخ آخرین به‌روزرسانی	2020 June 3 16:00 GMT
توضیحات	آسیب‌پذیری در اجرای کانال بین VM نرم افزار Cisco IOS برای روترهای Cisco 809 و ۸۲۹ Industrial Integrated Services Routers (ISR صنعتی) و Cisco 1000 Series Connected Grid Routers (CGR1000) می‌تواند به مهاجم اجازه دهد دستورات شل دلخواه را در سرور مجازی دستگاه (VDS) اجرا کند.
محصولات آسیب‌پذیر	Cisco 809 and 829 Industrial ISRs CGR1000
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-udp-vds-inj-f2D5Jzrt

۳ منبع

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