بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

رفع چندین آسیب‌پذیری بحرانی در محصولات سیسکو

خبر آسیب‌پذیری

شناسه سند	Maher_13990511-02
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۵/۱۱
طبقه‌بندی سند	**عادی**

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

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ مقدمه

شرکت سیسکو در تاریخ ۲۹ جولای سال ۲۰۲۰، با انتشار چند بروزرسانی امنیتی، چندین آسیب‌پذیری را وصله زد؛ این آسیب‌پذیری‌ها با شناسه‌های CVE-2020-3382، CVE-2020-3375 و CVE-2020-3374 به ترتیب مربوط به دور زدن فرآیند احراز هویت، سرریز بافر و دورزدن فرآیند تخصیص منابع می‌باشند؛ علاوه بر این شرکت سیسکو در تاریخ ۱۷ جون سال ۲۰۲۰ برای برخی آسیب‌پذیری‌های بحرانی مربوط به Treck IPstack، با شناسه‌های CVE-2020-11896 تا CVE-2020-11914، بروزرسانی v1.7 را منتشر کرد[1,6].

این شرکت به روزرسانی‌های امنیتی دیگری را برای رفع ۸ آسیب‌پذیری با شدت بالا و متوسط که بر روی چندین نسخه نرم افزار DCNM[1] تأثیر می‌گذارند، منتشر کرد[1,2] ، شناسه این آسیب‌پذیری‌ها

CVE-2020-3377, CVE-2020-3384, CVE-2020-3383, CVE-2020-3386, CVE-2020-3376, CVE-2020-3460, CVE-2020-3462, CVE-2020-3461

می‌باشد.

۲ جزئیات فنی

- **CVE-2020-3375**

این آسیب‌پذیری با شدت بحرانی و Base Score ۹,۸ نرم‌افزار Cisco SD-WAN Solution Software را تحت تأثیر قرار می‌دهد و به مهاجم اجازه می‌دهد تا منجر به سرریز بافر از راه دور بر روی دستگاه‌های تحت تأثیر شود، در واقع این آسیب‌پذیری ناشی از اعتبارسنجی نادرست ورودی می‌باشد. مهاجم غیر مجاز با ارسال ترافیک ساختگی به یک دستگاه تحت تأثیر این آسیب‌پذیری، می‌تواند آن را اکسپلویت کرده و پس از اکسپلویت موفقیت‌آمیز این آسیب‌پذیری، می‌تواند به اطلاعاتی که مجوز دسترسی به آن‌ها را ندارد دسترسی پیدا کرده، تغییراتی را در سیستم اعمال کند که در واقع مجاز به انجام آن‌ها نیست و دستوراتی را با سطح دسترسی root در سیستم تحت تأثیر این آسیب‌پذیری اجرا کند[3].

این آسیب‌پذیری در صورت اجرای یک نسخه آسیب‌پذیر از نرم‌افزار Cisco SD-WAN Solution بر روی محصولات زیر تأثیر خواهد گذاشت[3]:

- IOS XE SD-WAN Software

[1] Cisco Data Center Network Manager

- SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Cloud Routers
- SD-WAN vEdge Routers
- SD-WAN vManage Software
- SD-WAN vSmart Controller Software

مشتریانِ محصولات سیسکو هر چه سریع‌تر، نرم‌افزارهای موجود در جدول ۱ تا جدول ۳ را به نسخه وصله شده ارتقاء دهند.

جدول ۱: نسخه‌های وصله شده نرم‌افزار Cisco SD-WAN vManage Software برای آسیب‌پذیری با شناسه CVE-2020-3375

First Fixed Release	Cisco SD-WAN vManage Software Release
ارتقاء به نسخه وصله شده قبلی	18.3.0
18.4.5	18.4.0
19.2.3	19.2.0
ارتقاء به نسخه وصله شده قبلی	19.3.0
20.1.1	20.1.0

جدول ۲: نسخه وصله شده نرم‌افزارهای Cisco SD-WAN vEdge, vBond و vSmart برای آسیب‌پذیری با شناسه CVE-2020-3375

First Fixed Release	Cisco SD-WAN vEdge, vBond and vSmart Software Releases
ارتقاء به نسخه وصله شده قبلی	18.3.0
18.4.5	18.4.0
19.2.3	19.2.0
ارتقاء به نسخه وصله شده قبلی	19.3.0
20.1.1	20.1.0

جدول ۳: نسخه‌های وصله شده نرم‌افزار Cisco IOS XE SD-WAN برای آسیب‌پذیری با شناسه CVE-2020-3375

First Fixed Release	Cisco IOS XE SD-WAN Software Release
ارتقاء به نسخه وصله شده قبلی	16.9
ارتقاء به نسخه وصله شده قبلی	16.10
ارتقاء به نسخه وصله شده قبلی	16.11
16.12.4	16.12
17.2.1r	17.2

- **CVE-2020-3374**

این آسیب‌پذیری با شدت بحرانی و Base Score ۹,۹ در رابط مدیریت مبتنی بر وب نرم‌افزار Cisco SD-WAN vManage وجود دارد و به مهاجم اجازه می‌دهد تا از راه دور، فرآیند تخصیص منابع را دور زده و به اطلاعات حساس دسترسی پیدا کند، پیکربندی سیستم را تغییر دهد و به سیستم تحت تأثیر، لطمه بزند. این

آسیب‌پذیری در واقع ناشی از بررسی نادرست دسترسی و تخصیص منابع[۲] در سیستم تحت تأثیر این آسیب‌پذیری می‌باشد. مهاجم می‌تواند با ارسال یک درخواست HTTP ساختگی به رابط مدیریت مبتنی بر وبِ دستگاه تحت تأثیر، این آسیب‌پذیری را اکسپلویت کند؛ پس از اکسپلویت موفقیت‌آمیز این آسیب‌پذیری، مهاجم فراتر از حد معمول، اجازه پیکربندیِ تخصیص منابع کاربران را خواهد داشت[4].

گفتنی است این آسیب‌پذیری در صورت اجرای یک نسخه آسیب‌پذیر از نرم‌افزار Cisco SD-WAN vManage بر روی دستگاه‌های سیسکو تأثیر خواهد گذاشت و به مشتریانِ محصولات سیسکو توصیه می‌شود هر چه سریع‌تر، نرم‌افزارهای موجود در جدول ۴ را به نسخه وصله شده ارتقاء دهند.

جدول ۴نسخه‌های وصله شده نرم‌افزارCisco SD-WAN vManage Software برای آسیب‌پذیری با شناسه CVE-2020-3374

First Fixed Release	Cisco SD-WAN vManage Software Release
ارتقاء به نسخه وصله شده قبلی	Earlier than 18.3
ارتقاء به نسخه وصله شده قبلی	18.3
18.4.5	18.4
19.2.2	19.2
ارتقاء به نسخه وصله شده قبلی	19.3
20.1.1	20.1

- **CVE-2020-3382**

این آسیب‌پذیری با شدت بحرانی و Base Score ۹,۸ در REST API مربوط به نرم افزار Data Center Network Manager (DCNM) شرکت سیسکو، به یک مهاجم غیر مجاز اجازه می‌دهد تا از راه دور فرآیند احراز هویت را دور زده و کدهای دلخواه خود را با سطح دسترسی administrative بر روی دستگاه آسیب‌پذیر اجرا کند. این آسیب‌پذیری ناشی از نصب‌های مختلفی است که دارای یک کلید رمزگذاری استاتیک هستند. مهاجم می‌تواند آسیب‌پذیری مذکور را با استفاده از کلید استاتیک برای ایجاد یک توکن session معتبر، اکسپلویت نماید. مهاجم پس از یک اکسپلویت موفق می‌تواند اقدامات دلخواه خود را از طریق REST API با سطح دسترسی administrative انجام دهد [5]:

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,

[۲] insufficient authorization checking

CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914 (Cisco Bug IDs: CSCvu68945)

آسیب‌پذیری‌های موجود در اجرای Treck IP stack در مجموع با عنوان Ripple20 شناخته می‌شوند. اکسپلویت این مجموعه آسیب‌پذیری‌ها بسته به یک آسیب‌پذیری خاص، می‌تواند منجر به حملات اجرای کد از راه دور، انکار سرویس یا افشای اطلاعات شود [2, 6]. تیم واکنش به حوادث امنیتی سیسکو اعلام کرده است که از هر گونه سوءاستفاده مخرب از این آسیب‌پذیری‌ها اطلاعی ندارد [2, 6] .

آسیب‌پذیری مذکور، تمام حالت‌های راه‌اندازی دستگاه‌های DCNM سیسکو که با استفاده از ova. و iso. installer نصب شده‌اند را تحت تاثیر قرار می‌دهد. نسخه‌های آسیب‌پذیر نرم‌افزار DCNM عبارتند از: 11.0(1)، 11.1(1)، 11.2(1) و 11.3(1). با تایید شرکت سیسکو، آسیب‌پذیری ذکر شده نرم‌افزار DCNM را که با استفاده از DCNM installer برای سیستم‌عامل‌های ویندوز و لینوکس بر روی سیستم‌عامل‌های customer-provided نصب شده‌اند، تحت تاثیر قرار نمی‌دهد. این شرکت همچنین تایید کرده است که نسخه‌های 7.x و 10.x تحت تاثیر این آسیب‌پذیری قرار نمی‌گیرند.

سیسکو آسیب‌پذیری فوق را با انتشار نسخه 11.4(1) و بالاتر نرم‌افزار DCNM رفع و وصله کرده است. جهت دانلود این نرم‌افزار از Software Center در Cisco.com، مراحل زیر را دنبال کنید:

- بر روی Browse All کلیک کنید.
- Cloud and Systems Management > Data Center Infrastructure Management > Data Center Network Manager را انتخاب کنید.
- از پنل سمت چپ Data Center Network Manager در این صفحه، یک نسخه را انتخاب کنید.

۳ محصولات تحت تأثیر

به طور کلی این آسیب‌پذیری‌ها چندین محصول سیسکو را تحت تاثیر قرار می‌دهند که عبارتند از:

- IOS XE SD-WAN Software [3, 4]
- SD-WAN vBond Orchestrator Software [3, 4]
- SD-WAN vEdge Cloud Routers [3]
- SD-WAN vEdge Routers [3, 4]
- SD-WAN vManage Software [3]
- SD-WAN vSmart Controller Software [3, 4]
- DCNM software releases 11.0(1), 11.1(1), 11.2(1), and 11.3(1) [5]
- ASR 5000 [6]
- ASR 5500 [6]
- Virtual Packet Core [6]
- StarOS Software [6]

۴ توصیه امنیتی

سیسکو چندین بروزرسانی نرم‌افزاری جهت رفع آسیب‌پذیری‌های بحرانی با شناسه‌های CVE-2020-3375، CVE-2020-3374 و CVE-2020-3382 و همچنین آسیب‌پذیری‌هایی با شدت بالا و متوسط را به صورت رایگان منتشر کرده است [1]. CERT-EU به کاربران توصیه می‌کند با توجه به شدت و اهمیت آسیب‌پذیری‌های عنوان شده که در اسرع وقت نسبت اعمال به بروزرسانی‌های منتشر شده اقدام نمایند.

۵ منابع

[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://www.bleepingcomputer.com/news/security/cisco-fixes-severe-flaws-in-data-centermanagement-solution/

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdbufof-h5f5VSeL

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uabvman-SYGzt8Bv

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypassdyEejUMs

[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC