بسمه تعالی

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

۱۹ آسیب پذیری روز صفربا نامRipple20

اخبار آسیب‌پذیری

شناسه سند	Maher_13990401-1
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۴/۰۱
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 خلاصه

آزمایشگاه تحقیقاتی JSOF مجموعه‌ای از آسیب‌پذیری‌های روز صفر را در یک کتابخانه نرم‌افزاری سطح پایین TCP/IP توسعه داده شده توسط Treck Inc، که بسیار نیز مورد استفاده قرار می‌گیرد کشف کرده است. ۱۹ آسیب‌پذیری با نام Ripple۲۰، صدها میلیون دستگاه (یا بیشتر) را تحت تاثیر قرار داده است و شامل چندین آسیب‌پذیری اجرای کد از راه دور می‌باشد. از جمله خطرات این آسیب‌پذیری‌ها می توان به سرقت داده‌ها از یک پرینتر، اختلال در عملکرد دستگاه‌های کنترل صنعتی، حمله انکار سرویس(DoS) و افشای اطلاعات اشاره کرد. یک مهاجم می‌تواند سال‌ها کد مخرب را در دستگاه‌های جداسازی‌شده پنهان کند. یکی از این آسیب‌پذیری‌ها می‌تواند ورود به مرزهای شبکه را از خارج فعال کند.

نرم افزار شبکه‌ای Treck IP Stack برای انواع مختلف سیستم‌ها طراحی و ساخته شده است، این نرم‌افزار شامل چندین آسیب‌پذیری است که اکثر آن‌ها به دلیل نقص‌های موجود در مدیریت حافظه می‌باشند. گستردگی کاربرد این نرم افزار در بخش های مختلف که برخی از آنها در شکل ۱ اشاره شده است، نگرانی‌ها را در بین فعالان امنیت سایبری بالا برده است.

شکل ۱) حوزه‌های کاربردی که کتابخانه آسیب پذیر Treck stack در آنها به کار می‌رود

۲ توضیحات فنی

Ripple20 مجموعه‌ای از ۱۹ آسیب‌پذیری است که در Treck TCP/IP stack کشف شده اند که چهار مورد از آن‌ها دارای امتیاز CVSS بیش از ۹ هستند و از طریق اجرای کد دلخواه از راه دور فعال می‌شوند. یکی از آسیب‌پذیری‌های مهم، نقص در پروتکل DNS می‌باشد که ممکن است از طریق اینترنت و توسط یک مهاجم ساختگی، خارج از مرزهای شبکه، حتی در دستگاه‌هایی که به اینترنت متصل نیستند، اکسپلویت شود.

دومین Whitepaper که به دنبال BlackHat USA2020 منتشر می‌شود، جزئیات اکسپلویت آسیب‌پذیریِ CVE-2020-11901، یعنی نقص DNS بر روی یک دستگاه Schneider Electric APC UPS را ارائه می‌دهد. ۱۵ آسیب‌پذیری دیگر دارای CVSSهای ۳,۱ تا ۸,۲ می‌باشند که از طرق مختلف از جمله حمله انکار سرویس و اجرای کد دلخواه از راه دور، فعالیت خود را انجام می‌دهند. بسیاری از این آسیب‌پذیری‌ها به دلیل داشتن قابلیت تغییر کد و پیکربندیStack، در اثر گذر زمان دارای چندین نوع مختلف می‌باشند؛ همچنین آسیب‌پذیری‌های Ripple20، به دلیل داشتن اثر زنجیره‌ای و آن که به مهاجمان اجازه می‌دهند NAT و فایروال‌ها را دور زده و بدون نیاز به دخالت هیچ کاربری کنترل دستگاه‌ها را به دست گیرند، در نوع خود منحصر به فرد می‌باشند.

۳ ارزیابی خطر و کاهش آن

۳-۱ اعمال به‌روزرسانی‌ها

نرم‌افزار Treck IP stack باید به آخرین نسخه منتشر شده به‌روزرسانی شود (6.0.1.67 یا بالاتر).

اولین و بهترین راه‌حل، اعمال وصله‌های منتشر شده برای همه دستگاه‌ها می‌باشد. اگر اعمال وصله‌ها امکان‌پذیر نبود، اقدامات زیر انجام شود:

- قرار گرفتن در معرض شبکه برای دستگاه‌های حساس را به حداقل رسانده و دسترسی به اینترنت فقط در صورت نیاز انجام شود.
- تفکیک شبکه‌ها و دستگاه‌های OT در پشت firewall و جداسازی آن‌ها از شبکه تجاری.
- روش‌های دسترسی ایمن از راه دور فعال شود.

۳-۲ تشخیص و مسدود کردن ترافیک آی پی غیر فعال

حملات شبکه باید با بررسی بسته‌ها مسدود شوند. در برخی موارد، سوئیچ‌های مدرن، روتر و فایروال‌ها، بسته‌های ناقص و بدون تنظیمات اضافی را رها می‌کنند؛ توصیه می‌شود این تنظیمات امنیتی فعال باشند. در زیر لیستی از راه‌حل‌های احتمالی وجود دارد که می‌توانند متناسب با محیط شبکه اعمال شوند:

- در صورت عدم پشتیبانی در محیط شبکه، نرمال سازی یا مسدود کردن قطعات IP انجام شود.
- مسدود یا غیرفعال سازی یا IP tunneling (IPv6-in-IPv4 یا IP-in-IP tunneling) در صورت لزوم.
- مسیریابی منبع IP مسدود شده و ویژگی‌های IPv6 کم ارزش مانند هدرهای مسیریابی VU # 267289 حذف شود.
- بررسی TCP و حذف بسته‌های TCP ناقص.
- مسدود کردن پیام‌های کنترل نشده ICMP، مانند به‌روزرسانی MTU و به‌روزرسانی‌های آدرس mask
- عادی سازی DNS از طریق یک سرور بازگشتی امن یا فایروال لایه برنامه.
- ایجاد امنیت در DHCP / DHCPv6 با امکاناتی مانند DHCP snooping.
- مسدود یا غیرفعال سازی قابلیت‌های multicast IPv6.
- غیرفعال کردن DHCP برای IPهای استاتیک.
- قابل اطمینان بودن تجهیزات OSI لایه ۲ (Ethernet) بررسی شود.

۴ شرح آسیب پذیری ها

در جدول ۱، اطلاعات مربوط به آسیب‌پذیری‌هایی که توسط JSOF به CERT / CC گزارش داده شد را مشاهده می‌کنید.

جدول ۱: اطلاعات مربوط به هر یک از آسیب‌پذیری‌ها

CVE	CVSSv3	توضیحات	نسخه وصله شده
CVE-2020-11896	۱۰	این آسیب‌پذیری کار خود را با ارسال بسته‌های ناقص IPv۴ به دستگاهی که از تونل IPv۴ پشتیبانی می‌کند، شروع کرده و بر روی هر دستگاهی که Treck را با پیکربندی خاصی اجرا می‌کند تأثیر می‌گذارد و همچنین امکان اجرای کد دلخواه از راه دور را برای مهاجم فراهم می‌آورد.	۳۰ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11897	۱۰	این آسیب‌پذیری با ارسال چندین بسته ناقص IPv۶ به یک دستگاه، شروع به کار می‌کند و با اجرای کد دلخواه از راه دور،	۴ژوئن ۲۰۰۹ نسخه 5.0.1.35

CVE	CVSSv3	توضیحات	نسخه وصله شده
		بر روی تمامی نسخه‌های قدیمی Treck که IPv۶ را پشتیبانی می‌کنند، تأثیر می‌گذارد.	
CVE-2020-11901	۹	این آسیب‌پذیری کار خود را پاسخ به درخواست DNS شروع می‌کند و بر هر دستگاهی که Treck را با پشتیبانی از DNS اجرا می‌کند تأثیر می‌گذارد. از این آسیب‌پذیری می‌توان جهت اجرای کد دلخواه از راه دور بر روی Schneider Electric APC UPS سوءاستفاده کرد و علیرغم آنکه دارای CVSS۹,۰ است، اما از نظر ما در بین آسیب‌پذیری‌های مطرح شده، شدیدترین نوع آن‌ها به حساب می‌آید، به دلیل آنکه ممکن است درخواست‌های DNS از شبکه‌ای که دستگاه در آن قرار دارد، خارج شود و مهاجم بتواند از طریق حافظه نهان DNS و یا سایر روش‌ها جهت احاطه دستگاهی خارج از شبکه، از این آسیب‌پذیری سوءاستفاده کرده، به شبکه نفوذ کند و کنترل دستگاه را با دور زدن اقدامات امنیتی، در اختیار گیرد.	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11898	۹,۱	دستکاری نادرست پارامتر طول(CWE-130) در مؤلفه IPv4/ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11900	۸,۲	امکان Double Free (CWE-۴۱۵) در مؤلفه IPv4 هنگام ارسال بسته توسط مهاجم شبکه.	۱۵ اکتبر ۲۰۱۴ نسخه 6.0.1.41
CVE-2020-11902	۷,۳	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6OverIp4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11904	۵,۶	امکان Overflow یا Wraparound در مؤلفه تخصیص حافظه (CWE-190) هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان نوشتن خارج از محدوده (CWE-787).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11899	۵,۴	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه، امکان خواندن خارج از محدوده (CWE-125) و امکان حمله انکار سرویس.	۳ مارس ۲۰۲۰ نسخه 6.0.1.66

CVE	CVSSv3	توضیحات	نسخه وصله شده
CVE-2020-11803	۵,۳	امکان خواندن خارج از محدوده (CWE-125) در مؤلفه DHCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۱۰ اکتبر ۲۰۱۰ نسخه 6.0.1.28
CVE-2020-11905	۵,۳	امکان خواندن خارج از محدوده (CWE-125) در مؤلفه DHCPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11906	۵	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه Ethernet Link Layer از بسته‌ای که توسط یک کاربر غیر مجاز ارسال شده است و همچنین امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11907	۵	دستکاری نادرست پارامتر طول(CWE-130) در مؤلفه TCP از بسته‌ای که توسط یک کاربر غیر مجاز ارسال شده است و همچنین امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11909	۳,۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان Underflow (CWE-191)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11910	۳,۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125)	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11911	۳,۷	امکان کنترل دسترسی در مؤلفه ICMPv4 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و اختصاص مجوز درسترسی نادرست به منابع بحرانی(CWE-723).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11912	۳,۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه TCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11913	۳,۷	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه IPv6 هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66
CVE-2020-11914	۳,۱	اعتبارسنجی نامناسب ورودی (CWE-۲۰) در مؤلفه ARP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان خواندن خارج از محدوده (CWE-125).	۳ مارس ۲۰۲۰ نسخه 6.0.1.66

CVE	CVSSv3	توضیحات	نسخه وصله شده
CVE-2020-11908	۳,۱	امکان Null Termination (CWE-۱۷۰) در مؤلفه DHCP هنگام ارسال بسته توسط مهاجم غیرمجاز شبکه و امکان افشای اطلاعات حساس(CWE-200).	۱۱ آگوست ۲۰۰۷ نسخه 4.7.1.27

۵ محصولات آسیب پذیر و تحت تاثیر

همانطور که در بخش های قبلی اشاره شد، این آسیب پذیری طیف گسترده ای از محصولات را شامل می شود. فهرستی از محصولات تحت تاثیر قرار گرفته بصورت دقیق و با تماس هایی که CISA ICS-CERT با تولید-کنندگان محصولات داشته است، تهیه شده است. بدیهی است این محصولات آسیب پذیر محدود به این لیست نمی باشد و ممکن است در آینده مورد بررسی مجدد قرار گیرد. جدول شماره ۲ نام شرکتهایی را نشان میدهد که وجود آسیب پذیری در محصولات خود را تایید کرده‌اند. در این فهرست نام شرکت‌های بزرگی چون Cisco، Intel، Caterpilar و HP به چشم می‌خورد.

جدول 2: فهرست شرکتهایی که وجود آسیب‌پذیری در محصولات خود را پذیرفته‌اند

STATUS: CONFIRMED (15)
B. Braun
Baxter
Caterpillar
Cisco (through Starent)
Digi
Green Hills
HCL Tech
HP
HPE
Intel
Maxlinear (through HLFN)
Rockwell
Sandia National Labs
Schneider Electric/APC
Teradici

لیست تأمین کنندگانی که ممکن است تحت تأثیر این آسیب‌پذیری قرار بگیرند در ذیل نمایش داده می‌شود:

جدول 3: فهرست شرکتهایی که وجود آسیب‌پذیری در محصولات خود را پذیرفته‌اند

STATUS: PENDING (57)		
EMC (now Dell)	Hitachi europe	SAIC
GE general electric (through quadros)	Hlfn	ScriptPro
NASA	Honeywell	Semtech
Verifone	Itron	Sigma Designs
Agilent	Kadak	SimCom Wireless
Airlinq(throug Netsnapper Technologies SARL)	L-3 Chesapeake Sciences Corporation	Starent Networks
Audiocodes	Lockheed martin	Synamedia(Through Cisco)/NDSUK
BAE systems	Marvell	Syncroness
BECK	Maxim Integrated Products	
Broadcom	Memjet	Thinkcom/ThinKom
Capsule (through digi)	MTS Technologies	Tollgrade communications
DASAN Zhone(through vpacket)	Netafim	Ultra Electronics Flightline Systems
Datamax Corporation	Netsnapper Technologies SARL	Vicom
Enghouse (through tollgrade communications)	NVIDIA (through portalplayer)	Videotek
Extreme Networks	Portalplayer	Vocera
Foundry	Qualstar.com	vpacket(now DASAN Zhone)
Fraunhofer IZFP	Quadros	Weibel weibel.dk
Gainspan (telit)	Red lion controls	Western geco
Guidant medical	Redcom	Xilinx
		Zodiac Aerospace

تأمین کنندگانی که ممکن است تحت تأثیر این آسیب‌پذیری قرار گیرند.

تجهیزات شبکه سیسکو که در کشور ما ایران نیز مورد استفاده قرار می گیرند تحت تاثیر این آسیب پذیری قرار گرفته اند. با توجه به اهمیت موضوع در بخش بعدی وضعیت محصولات Cisco مورد بررسی قرار گرفته است. از دیگر محصولات مهم که بصورت گسترده در کشور ایران مورد استفاده قرار می‌گیرد، چاپگرهای HP و Samsung می‌باشند که طبق اعلام شرکت سازنده تحت تاثیر این آسیب‌پذیری بوده و توصیه اکید می‌گردد مدیران شبکه نسبت به نصب بروزرسانی‌ها اقدام نمایند. فهرست محصولات و نحوه بروزرسانی در پیوند زیر قابل دسترسی می باشد.

https://support.hp.com/us-en/document/c06640149

۱-۵ وضعیت محصولات سیسکو

شرکت سیسکو در حال بررسی خط تولید خود می‌باشد تا مشخص کند که کدام یک از محصولاتش ممکن است تحت تأثیر این آسیب‌پذیری‌ها قرار گیرند که پس از بررسی‌های صورت گرفته، به هر یک از محصولات تحت تأثیر، یک شناسه نقص[۱] سیسکو اختصاص داده شد. این نقص‌ها از طریق Cisco Bug Search Tool قابل دسترسی بوده و حاوی اطلاعات تکمیلی از جمله راه‌حل‌ها[۲] (در صورت وجود) و نسخه‌های وصله شده نرم‌افزار می‌باشد. شایان ذکر است هر محصول یا سرویسی که در لیست محصولاتِ تحت تأثیر یا آسیب‌پذیر ذکر نشده باشد، آسیب‌پذیر تلقی نخواهد شد، اما از آنجا که بررسی‌ها کماکان در حال انجام می‌باشد، لذا ممکن است محصولاتی که در حال حاضر آسیب‌پذیر در نظر گرفته نشده‌اند، متعاقباً در لیست محصولات آسیب‌پذیر قرار گیرند.

محصولات زیر نیز، در حال بررسی می‌باشند تا مشخص شود که آیا آن‌ها نیز تحت تأثیر این آسیب‌پذیری قرار دارند یا خیر.

- 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

در جدول ۳ لیستی از محصولات آسیب‌پذیر شرکت سیسکو را ملاحظه می‌کنید. گفتنی است که اگر هیچ تاریخ و یا نسخه‌ای برای مولفه تحت تحت تأثیر ذکر نشده باشد، به این معناست که شرکت سیسکو در حال ادامه بررسی می‌باشد و در صورت دسترسی به اطلاعات تکمیلی، این اطلاعات نیز بروزرسانی خواهند شد و پس از نهایی شدن آن‌ها، مشتریان باید به بخش نقص(های) مرتبط سیسکو مراجعه نمایند.

جدول 4: محصولات آسیب‌پذیر شرکت سیسکو

محصول	شناسه نقص
Cisco GGSN Gateway GPRS Support Node	CSCvu60310
Cisco MME Mobility Management Entity	CSCvu60314
Cisco PGW Packet Data Network Gateway	CSCvu60313
Cisco System Architecture Evolution Gateway (SAEGW)	CSCvu60314

[۱] هر نقصی دارای یک unique identifier یا همان شناسه منحصر بفرد می‌باشد.

[۲] workarounds

گفتنی است فقط محصولاتی که در بخش محصولات آسیب‌پذیرِ شرکت سیسکو ، یعنی Vulnerable Products لیست شده‌اند، تحت تأثیر این آسیب‌پذیری‌ها قرار می‌گیرند. جهت کسب اطلاعات بیشتر در خصوص محصولات وصله شده نیز باید به همین بخش مراجعه کنید.

همواره به مشتریان توصیه می‌شود که پیش از ارتقاء نسخه یک نرم‌افزار، به صفحه مشاوره‌های امنیتی سیسکو _Cisco Security Advisories_ مراجعه کرده و از نظرات آن‌ها استفاده کنند. در کلیه موارد نیز مشتریان باید اطمینان حاصل کنند که دستگاه‌ها، دارای حافظه کافی بوده و پیکربندی‌های نرم‌افزار با نسخه جدید پشتیبانی شود و اگر در این زمینه اطلاعات کافی ندارند پیشنهاد می‌شود با مرکز خدمات فنی سیسکو (TAC[۳]) و یا پشتیبان‌های مربوطه تماس حاصل نمایند.

۶ ارزیابی ریسک و اقدامات پیشگیرانه

Ripple20 خطرات قابل توجهی را ایجاد می‌کند. از جمله آنها می‌توان به موارد زیر اشاره کرد:

- اگر مهاجمی خارج از شبکه باشد، در صورت دسترسی به اینترنت می‌تواند دستگاهی را در داخل شبکه کنترل کند.
- مهاجمی که قبلاً موفق به نفوذ به یک شبکه شده است می‌تواند از آسیب‌پذیری‌های این کتابخانه برای هدف قرار دادن دستگاه‌های خاص درون آن استفاده کند.
- یک مهاجم می‌تواند حمله‌ای را انتشار دهد که بتواند تمام دستگاه‌های آسیب‌دیده در شبکه را به طور همزمان در اختیار بگیرد.
- مهاجم ممکن است از دستگاه آسیب‌دیده به عنوان راهی برای پنهان ماندن در شبکه برای چندین سال استفاده کند.
- یک مهاجم در حالت پیشرفته‌تر به طور بالقوه می‌تواند خارج از مرزهای شبکه، حمله‌ای را بر روی دستگاهی در داخل شبکه انجام دهد و بنابراین پیکربندی‌های NAT را دور زند. این کار با انجام یک حمله MITM یا یک dns cache poisoning انجام می‌شود.
- در برخی از سناریوها، مهاجم ممکن است با پاسخ دادن به بسته‌هایی که مرزهای شبکه را رها می‌کنند، حملات خود را در خارج از شبکه و با دور زدن NAT انجام دهد.

[۳] Cisco Technical Assistance Center

در تمام سناریوهای ذکر شده، مهاجم می‌تواند بدون نیاز به تعامل کاربر، کنترل کاملی را از راه دور بر روی دستگاه مورد نظر بدست آورد.

JSOF توصیه می‌کند که اقدامات لازم را برای به حداقل رساندن یا کاهش خطر بهره‌برداری از دستگاه انجام دهید. گزینه‌های انتخابی جهت کاهش خطرات، به بستر موجود بستگی دارد. به طور کلی انجام مراحل زیر توصیه می‌شود:

- تمام سازمان‌ها قبل از اعمال اقدامات لازم، باید یک ارزیابی جامع از مخاطرات احتمالی را انجام دهند. ابتدا اقدامات دفاعی را در حالت غیرفعال "alert" گسترش دهید.
- اقدامات مربوط به فروشندگان دستگاه:
  - مشخص کنید که آیا از یک Treck stack آسیب‌پذیر استفاده می‌کنید یا خیر
  - ارتباط با Treck برای اطلاع از خطرات موجود
  - برزورسانی به آخرین نسخه Treck stack (۶,۰,۱,۶۷ و بالاتر)
  - در صورت عدم امکان بروزرسانی، در صورت امکان غیرفعال کردن featureهای آسیب‌پذیر را در نظر بگیرید
- اقدامات مربوط به اپراتورها و شبکه‌ها:
  - اولین و بهترین اقدام، بروزرسانی به نسخه‌های وصله شده است. در صورت بروزرسانی دستگاه‌ها، مراحل زیر توصیه می‌شود:
    - قرار گرفتن در معرض شبکه برای دستگاه‌های بحرانی و حساس را به حداقل رسانده مگر در موارد ضروری و اطمینان حاصل کنید که دستگاه‌ها از طریق اینترنت در دسترس نیستند مگر اینکه قطعا ضروری باشد.
    - شبکه‌ها و دستگاه‌های OT را در پشت فایروال‌ها جدا کرده و آنها را از شبکه تجاری جدا کنید.
    - تنها روش‌های امن دسترسی از راه دور را فعال کنید.
  - ترافیک غیرعادی IP را مسدود کنید
  - حملات شبکه را از طریق بررسی deep packet ها مسدود کنید تا خطرات مربوط به دستگاه‌های Treck فعال شده با TCP/IP خود را کاهش دهید.

فیلتر کردن ترافیک Pre-emptive، روش موثری است که می‌تواند متناسب با محیط شبکه شما اعمال شود. گزینه‌های فیلتر شامل موارد زیر می‌شوند:

- IP fragments ها را مسدود یا نرمال‌سازی کنید.
- در صورت لزوم، IP tunneling (IPv6-in-IPv4 یا IP-in-IP tunneling) را مسدود یا غیرفعال کنید.

- مسیریابی منبع IP و هر ویژگی کم ارزش IPv6 مانند مسیریابی هدرهای VU#267289 را مسدود کنید.
- پیام‌های استفاده نشده کنترل ICMP مانند بروزرسانی MTU و بروزرسانی Address Mask را مسدود کنید.
- DNS را از طریق یک سرور بازگشتی ایمن یا فایروال بازرسی DNS، نرمال‌سازی کنید. (بررسی کنید که سرور DNS بازگشتی شما درخواست‌ها را نرمال‌سازی می‌کند)
- امنیت DHCP/DHCPv6 را با ویژگی‌هایی مانند DHCP snooping بالا ببرید.
- در صورتیکه از قابلیت‌های multicast یا چندبخشی IPv6 در زیرساخت switching استفاده نمی‌شود، آن را غیرفعال یا مسدود کنید.
- در جایی که IPهای استاتیک قابل استفاده هستند، DHCP را غیرفعال کنید.
- IDS and IPS signatures های شبکه را بکار بگیرید.
- در صورت وجود، segmentation شبکه را انجام دهید.

با توجه به اینکه در کشور ایران نمایندگی رسمی شرکت‌های تحت تاثیر این آسیب‌پذیری مشغول به فعالیت نمی‌باشند، این وظیفه مدیران و کارشناسان شبکه سازمان‌هاست که در اولین فرصت نسبت به بررسی و بروزرسانی firmware محصولات مذکور اقدام نمایند. توصیه می‌شود هر چه سریع‌تر نرم‌افزار Treck IP stack را به آخرین نسخه آن (۶,۰,۱,۶۷ یا بالاتر) بروزرسانی کنید. همچنین پیشنهاد می‌گردد حملات شبکه را از طریق deep packet inspection مسدود کنید، در برخی موارد سویچ‌ها، روترها و فایروال‌ها بسته‌های ناقص و بدون تنظیمات تکمیلی را رها می‌کنند. توصیه می‌شود چنین ویژگی‌های امنیتی غیرفعال نباشند.

۷ منابع

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

[2] https://www.jsof-tech.com/ripple20/

[3] https://www.kb.cert.org/vuls/id/257161

[4] https://support.hp.com/us-en/document/c06640149