بسمه تعالی

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

Ruleهای طراحی شده جهت تشخیص آسیب‌پذیری‌های Ripple20 و جلوگیری از حمله

سایر

شناسه سند ..... Maher_13990523-01
نوع سند ..... گزارش فنی
شماره نگارش ۱/۰
تاریخ نگارش ۱۳۹۹/۰۵/۲۲
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 مقابله با آسیب‌پذیری‌های Ripple20

پشته شبکه Treck TCP/IP به طور گسترده در بسیاری از سازمان‌ها و صنایع، به خصوص در بخش‌های مرتبط با دستگاه‌های IoT مستقر در سازمان‌ها، بخش‌های کنترل صنعت، مراقبت‌های بهداشتی و موارد دیگر مورد استفاده قرار می‌گیرد.

از زمان کشف زنجیره ۱۹ آسیب‌پذیری با نام Ripple20، سازمان‌های امنیتی به دنبال روش‌هایی برای محافظت سازمان خود در برابر این آسیب‌پذیری‌ها بوده‌اند. توسعه دهندگان در صنایع متفاوتی در تلاش‌اند تا وصله‌هایی را برای این نقض‌های امنیتی ارائه دهند. تولید این وصله‌ها به زمان زیادی نیاز دارد.

به بسیاری از این آسیب‌پذیری‌ها بر اساس عواملی از قبیل سختی بهره‌برداری، دسترسی محلی یا از راه دور و شدت تأثیر، شدت کمتری اختصاص یافت. با این حال چهار مورد از آن‌ها شدت بالایی داشته و به راحتی مورد بهره‌برداری قرار می‌گیرند. تأثیر این آسیب‌پذیری‌ها از حملات «انکار سرویس» تا بهره‌برداری «اجرای کد از راه دور از طریق اینترنت» متفاوت است.

به منظور تشخیص و جلوگیری از بهره‌برداری از چهار مورد از آسیب‌پذیری‌های بحرانی Ripple20 و حملات مرتبط با آن، متخصصان امنیتی در شرکت McAfee ATR با همکاری شرکت JSOF (کاشف این آسیب‌پذیری‌ها) روش‌هایی جهت تشخیص ماشین‌های آسیب‌پذیر و Ruleهای Suricata برای IDSها، طراحی کرده است.

Ruleهای مذکور در لینک زیر موجود است:

https://github.com/advanced-threat-research/Ripple-20-Detection-Logic/tree/master/suricata_rules

سازمان‌ها با استفاده از وصله‌های منتشر شده، پیاده‌سازی روش‌های تشخیص ماشین‌های آسیب‌پذیر با استفاده از راه‌حل‌های امنیتی شبکه یا ابزارهای متن‌باز بر اساس Ruleهای ارائه شده می‌توانند به درک بهتر و مقابله با این نقض‌های بحرانی دست یابند.

هنگام استفاده از Ruleهای مذکور شرایطی وجود دارد که با رعایت کردن آنها (برای هر آسیب‌پذیری) احتمال به وجود آمدن موارد False positive یا False negative کمتر خواهد بود. این شرایط به اختصار در ادامه شرح داده شده است. با این حال نسخه کامل‌تر در بخش «Recommended detection criteria» در لینک زیر آمده است:

https://github.com/advanced-threat-research/Ripple-20-Detection-Logic

۱. **CVE-2020-11901 (Variant 1):**

- دستگاه باید قادر به پردازش ترافیک DNS و پاسخ به درخواست‌ها در این بستر باشد.
- دستگاه باید قادر باشد هر نام دامنه را (example.com) در هر بسته DNS تشخیص دهد.
- دستگاه باید قادر باشد هر «پاسخ DNS»ی که اندازه‌اش از حد مورد انتظار بیشتر است را تشخیص دهد.
- دستگاه باید قادر باشد هر بسته‌ی DNSی که نام DNS آن از ۲۵۵ بایت (قبل از فشرده‌سازی) بیشتر باشد را تشخیص دهد.
- دستگاه باید قادر باشد هر «پاسخ DNS»ی که نام DNS آن حاوی کاراکتری‌هایی به جز «a تا z»، «A تا Z»، «۰ تا ۹»، «-»، «_» و «*» باشد را تشخیص دهد.
- دستگاه باید قادر باشد پاسخ‌های DNSی که تعداد زیادی اشاره‌گر فشرده‌سازی دارند را تشخیص دهد، به‌طور خاص اشاره‌گرهایی که پست سر هم آمده‌اند.

۲. **CVE-2020-11901 (Variant 2):**

- دستگاه باید قادر باشد پاسخ‌های DNS دریافتی را پردازش کند.
- دستگاه باید قادر باشد رکوردهای CNAME در پاسخ‌های DNS را تشخیص دهد.
- دستگاه باید قادر باشد همه‌ی پاسخ‌های DNSی که اندازه‌ی فیلد RDATAی موجود در رکورد CNAME آنها، بیشتر از حد تعیین شده در فیلد RDLENGTH در همان رکورد است، را تشخیص دهد.

۳. **CVE-2020-11897:**

- دستگاه باید قادر باشد ترافیک IPV6 فرگمنت شده را پردازش کند.
- دستگاه باید بسته‌های فرگمنت شده‌ی حاوی Routing Header type 0 (RH0) را بررسی کند.
- اگر اندازه بسته‌ی فرگمنت شده که حاوی RH0 است کمتر از اندازه‌ی گزارش شده در سرآیند مسیریابی باشد، احتمال دارد آسیب‌پذیری مورد بهره‌برداری قرار گرفته باشد.
- اگر با بازسازی بسته‌های فرگمنت شده، سرآیند لایه‌ی زیرین IPv6 به شکل ناقص ظاهر شود، ممکن است آسیب‌پذیری مورد بهره‌برداری قرار گرفته باشد.

۴. **CVE-2020-11896:**

اگر امکان باز کردن encapsulation داده وجود دارد، برای تشخیص حمله‌ای که در حال وقوع است شرایط زیر باید برقرار باشد:

- صف دریافتی UDP نباید خالی باشد.
- بسته‌های دریافتی UDP باید فرگمنت شده باشند.
- بسته‌های فرگمنت شده باید بسته‌های کپسوله شده IPv4 داشته باشند.

- بسته‌های کپسوله شده IPv4 باید بین دو قسمت از بسته تقسیم شوند.
- اندازه‌ی داده در سرآیند IP در بسته‌های سرهم‌شده‌ی IPv4 باید صحیح باشد.

اگر امکان باز کردن encapsulation داده وجود ندارد، برای تشخیص حمله‌ای که در حال وقوع است شرایط زیر باید برقرار باشد:

- صف دریافتی UDP نباید خالی باشد.
- بسته‌های دریافتی UDP باید فرگمنت شده باشند.
- طول کل فرگمنت در آخرین فرگمنت، از فیلد offset بیشتر باشد.

۲ ملاحظات خاص در استفاده از Ruleها

جهت استفاده از این ruleها، محدودیت‌هایی در مورد هر آسیب‌پذیری وجود دارد که در ادامه به اختصار شرح داده شده است:

- ملاحضات Ruleهای مربوط به آسیب‌پذیری CVE-2020-11901:

جهت تشخیص این آسیب‌پذیری باید طول همه نام‌های DNS موجود در درخواست‌های DNS دریافتی محاسبه گردد. محاسبه طول کلیه درخواست‌های DNS دریافتی دشوار است، به خصوص زمانی که هر درخواست حاوی نام‌های DNS بسیاری باشد.

در حال حاضر مشخص نیست که بهره‌برداری از این آسیب‌پذیری در صورت استفاده از EDNS(0) و یا DNS-over-TCP امکان پذیر است یا خیر. با این حال برای مقابله با این آسیب‌پذیری دو rule جهت تعیین اندازه DNS از طریق ترافیک TCP ایجاد شده است. لازم به ذکر است که rule دوم از TCP اولیه به جای DNS اولیه استفاده می‌کند.

- ملاحضات Ruleهای مربوط به آسیب‌پذیری CVE-2020-11897:

در هنگام پردازش بسته‌های دریافتی IPv6، بررسی سرآیند به جای اینکه تنها در بخش طول قطعه انجام شود در کلیه بسته‌ها صورت گرفته و سبب بروز خطا در تجزیه سرآیند در مسیریابی آدرس‌های IPv6 می‌شود. در حین بازسازی قطعه‌ها، آدرس‌های IPv6 با داده‌هایی از قطعات مربوطه پر می‌شود، که باعث به وجود آمدن آدرس‌های IPv6 نامعتبر در سرآیند و همچنین ایجاد نقص در لایه بعدی بسته می‌شود.

- ملاحضات Ruleهای مربوط به آسیب‌پذیری CVE-2020-11896:

این آسیب‌پذیری از مدیریت نادرست بسته‌های IPv4-in-IPv4 ورودی در Treck TCP/IP stack ناشی می‌شود. این مسئله می‌تواند امکان اجرای کد از راه دور را هنگام ارسال بسته‌های متعدد tunnel شده UDP به یک host آسیب‌پذیر فراهم کند. Treck stack حداقل دو سطح از tunneling را پشتیبانی می‌کند. هر مرحله از tunnel می‌تواند IPv4-in-IPv4، IPv6-in-IPv4 و IPv4-in-IPv6 باشد که در این بخش از IPv4-in-IPv4 و tunneling تک سطحی استفاده شده است.

۳ مراجع

[1] https://www.cryptobasenews.com/ripple/time-to-tame-the-ripple-effect/

[2] https://www.businesswire.com/news/home/20200805005078/en/McAfee-Advanced-Threat-Research-JSOF-Collaborate-Defend

[3] https://github.com/advanced-threat-research/Ripple-20-Detection-Logic