بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی آسیب‌پذیری‌های سیستم عامل بلادرنگ VxWorks

مهر ۹۸

فهرست مطالب

۱ چکیده

هنگامی‌که آسیب‌پذیری‌های عمده در سیستم‌عامل‌های معمول مانند ویندوز مایکروسافت پیدا می‌شود، با سوءاستفاده از این آسیب‌پذیری‌ها می‌توان میلیون‌ها دستگاه را تحت تأثیر قرار داد. در ماه جولای امسال تیم تحقیقاتی Armis، Armis Labs، 11 آسیب پذیری روز صفرم را در VxWorks، پرکاربردترین سیستم عامل مورد استفاده که ممکن است هرگز در مورد آن نشنیده باشید، کشف کرده اند. VxWorks در بیش از ۲ میلیارد دستگاه از جمله دستگاه‌های مهم صنعتی، پزشکی و سازمانی مورد استفاده قرار می‌گیرد. این آسیب-پذیری در پشته TCP/IP (IPnet) آن قرار دارد و بر روی همه نسخه‌های آن تا نسخه ۶.۵ تأثیر می‌گذارد و نمونه ای نادر از آسیب‌پذیری‌های موجود در سیستم‌عامل طی ۱۳ سال گذشته است. آرمیس با Wind River، پشتیبانی‌کننده VxWorks، همکاری نزدیکی داشته است و نسخه VxWorks 7 به عنوان آخرین نسخه که در تاریخ ۱۹ ژوئیه منتشر شد، دارای اصلاحاتی در مورد همه آسیب پذیری‌های کشف شده است.

این آسیب پذیری‌ها، که به طور جمعی به Urgent / 11 لقب گرفته‌اند، از دو نظر تعجب آور هستند. اول، حضور آنها در پروتکل‌های شبکه سیستم عامل - "TCP / IP (IPnet) stack"، که به دستگاه‌ها در اتصال به شبکه‌هایی مانند اینترنت کمک می‌کند - غیر عادی است. محققان و هکرها در دهه ۱۹۹۰ تعدادی از اشکالات و کرم‌ها را در این پیاده سازی‌های پروتکل کشف کردند، اما از آن زمان به بعد امنیت این مؤلفه اساسی تا حد زیادی در سطح جهانی استاندارد شده است. دوم، یافتن آسیب پذیری‌های امنیتی به ویژه موارد بحرانی در VxWorks بطور کلی بسیار نادر است. در حالی که این آسیب پذیری‌ها بسیار گسترده هستند، Armis و Wind River تأکید کرده‌اند که در آخرین نسخه VxWorks یا نسخه‌های "مجوز[1]" Wind River مانند VxWorks 653 و VxWorks Cert Edition حضور ندارند. این بدان معنی است که تاسیسات مهم زیرساختی مانند نیروگاه‌های هسته‌ای آسیب‌پذیر نیستند.

۲ معرفی سیستم‌عامل بلادرنگ VxWorks

VxWorks پرکاربردترین سیستم عامل بلادرنگ (RTOS) در جهان است. RTOS توسط دستگاه‌هایی مورد استفاده قرار می‌گیرد که نیاز به دقت و اطمینان بالایی دارند، مانند زیرساخت‌های مهم، تجهیزات شبکه، دستگاه‌های پزشکی، سیستم‌های صنعتی و حتی فضاپیماها. به این ترتیب، VxWorks برای اهداف بسیار

[1] Certification

گسترده ای استفاده می‌شود، از PLCها گرفته تا دستگاه‌های MRI، دیوار آتش و چاپگرها، هواپیماها، قطارها و موارد دیگر.

VxWorks که اولین با در سال ۱۹۸۷ منتشر شد، یکی از بالغ‌ترین سیستم عامل‌هایی است که هنوز هم به طور گسترده مورد استفاده قرار می‌گیرد و به دلیل ماهیت دستگاه‌هایی که با آن کار می‌کنند و مشکلات در به روزرسانی آنها، تعداد زیادی از نسخه‌های آن پشتیانی می‌شود. تا به حال تنها معدود آسیب‌پذیری‌هایی که روی این سیستم‌عامل تأثیر می‌گذارند، شناسایی شده بود و هیچکدام به اندازه URGENT / 11 بحرانی نبودند. ماهیت غیرقابل توصیف VxWorks از این واقعیت ناشی می‌شود که منبع بسته است، این امر بازرسی را دشوارتر می‌کند، و این واقعیت که این سیستم‌عامل از نوع RTOS است، باعث شده به دلیل عدم کاربرد مستقیم آن در دستگاه‌های مصرف کننده، از طرف جامعه پژوهشی مورد توجه کمتری قرار گیرد.

تحقیقات نشان می‌دهد RTOSها هم باید به اندازه دیگر نرم‌افزارها مورد بررسی قرار گیرند؛ زیرا هر نرم‌افزاری که مورد تحقیق قرار نگرفته باشد، دارای نقص هایی است که پس از کشف، ممکن است تأثیرات مخربی داشته باشد. عملکرد داخلی VxWorks نسبتاً در تاریکی باقی مانده است، و همینطور عیب‌های آن را نیز به دنبال داشته و منجر به آسیب پذیری‌های غیر عادی سطح پایین و یا بحرانی URGENT/11 شده است. از سوی دیگر RTOSها به دلیل دارا بودن سطح بالایی از قابلیت اطمینان، توسط دستگاه‌های مهم مورد استفاده قرار می‌گیرند. این امر باعث می‌شود اثر هرگونه آسیب پذیری که در آنها وجود دارد، بسیار سخت‌تر شود. مسلما غیرفعال کردن تلفن هوشمند برای هرکس ناخوشایند است، اما خاموش کردن یک کارخانه تولید داستانی کاملاً متفاوت خواهد بود!

علاوه بر این، دستگاه‌های VxWorks فاقد توانایی نصب یک عامل امنیتی هستند و تنها به تمامیت سیستم-عامل متکی هستند. VxWorks شامل برخی از موارد کاهشی اختیاری است که می‌تواند سوء استفاده از برخی آسیب پذیری‌های URGENT/11 را سخت کند؛ اما در حال حاضر دیده نشده که این تنظیمات مورد استفاده سازندگان دستگاه باشد. در دستگاه‌هایی که مورد بررسی قرار گرفته (و بهره برداری شده است)، تقریباً از هیچ یک از این کاهش‌ها از جمله ASLR، stack canaries و DEP استفاده نشده است. عدم وجود یک عامل امنیتی همراه با عدم استفاده از این موارد، آسیب پذیری‌های URGENT/11 را حتی خطرناک‌تر می‌کند.

۳ محصولات تحت تاثیر

همانطور که گفته شد، آسیب پذیری‌های URGENT/11 روی نسخه‌های VxWorks تا قبل از نسخه ۶.۵ تأثیر می‌گذارند، به استثنای نسخه‌های محصول طراحی شده برای صدور گواهینامه، مانند VxWorks 653 و VxWorks Cert Edition. لیست برخی از دستگاه‌های تحت تأثیر شامل موارد زیر است:

- دستگاه‌های SCADA
- کنترل‌کننده‌های صنعتی
- مانیتور بیمار
- دستگاه‌های MRI
- فایروال‌ها
- تلفن‌های VOIP
- چاپگرها

لیست برخی از شرکت‌ها یا دستگاه هایی نیز که از نسخه‌های VxWorks تحت تأثیر URGENT/11 استفاده می‌کنند، عبارتند از: ABB، Avaya، دستگاه‌های صنعتی Belden، Dräger، ExtremeNetworks، بهداشت و درمان GE، NetApp، فیلیپس، اتوماسیون Rockwell، اشنایدر الکتریک، زیمنس، فایروال‌های Sonicwall، TrendMicro IPS، وودوارد، پرینترهای زیراکس و Xylem.

از آنجایی که VxWorks معمولاً توسط بخش‌های صنعتی و بهداشتی مورد استفاده قرار می‌گیرد، هر دو آن-ها در معرض خطر فوق العاده‌ای از طرف آسیب پذیری‌های URGENT/11 قرار دارند. این خطر با توجه به ماهیت حساس دستگاه‌های VxWorks در چنین محیط‌هایی شدت می‌یابد. یک کنترلر صنعتی به خطر افتاده می‌تواند یک کارخانه را خاموش کند و یک مانیتور بیمار آلوده می‌تواند یک اثر تهدید کننده زندگی داشته باشد.

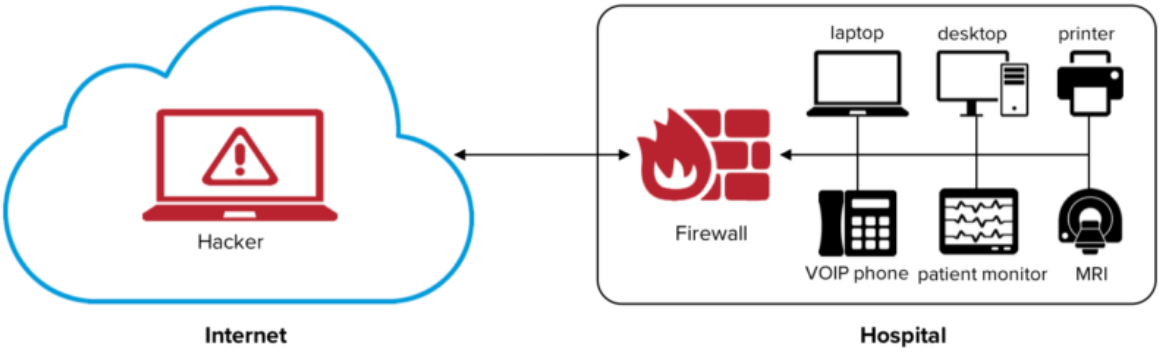
۴ تأثیر آسیب‌پذیری

URGENT / 11 خطرات قابل توجهی برای همه دستگاه‌های متصل VxWorks که در حال استفاده هستند، به وجود می‌آورد. بسته به موقعیت دستگاه در شبکه و موقعیت حمله کننده، سه سناریوی حمله وجود دارد. URGENT/11 می‌تواند توسط یک مهاجم برای کنترل دستگاهی که در محیط شبکه یا در داخل آن قرار دارد، استفاده شود. متناوباً، مهاجمی‌که قبلاً موفق به نفوذ در شبکه شده است، می‌تواند از URGENT/11 برای هدف قرار دادن دستگاه‌های خاص درون آن استفاده کند، یا حتی حمله ای را پخش کند که بتواند تمام دستگاه‌های تحت تأثیر VxWorks را در شبکه به طور همزمان هدف بگیرد. توجه به این نکته ضروری است که در همه سناریوها، یک مهاجم می‌تواند از راه دور و بدون نیاز به تعامل کاربر، کنترل کاملی را بر روی دستگاه مورد نظر بدست آورد و تفاوت فقط در نحوه دستیابی مهاجم به آن است.

شش مورد از آسیب پذیری‌ها به عنوان مهم و بحرانی طبقه بندی شده اند و امکان اجرای کد از راه دور (RCE) را فراهم می‌کنند. آسیب پذیری‌های باقی مانده به عنوان انکار سرویس، نشت اطلاعات یا نقص منطقی، طبقه بندی شده‌اند. آسیب‌پذیری‌های URGENT/11 جدی است؛ زیرا مهاجمان را قادر می‌سازد

کنترل دستگاه‌هایی را که نیاز به تعامل کاربر ندارند، به دست بیاورند و حتی دستگاه‌های امنیتی محیطی مانند فایروال‌ها و راه‌حل‌های NAT را نیز دور بزنند. این ویژگی‌های ویرانگر، آسیب پذیری‌های URGENT/11 را "کرم پذیر" می‌کند، به این معنی که می‌توان از آنها برای انتشار بدافزارها به داخل شبکه‌ها و نیز در داخل شبکه استفاده کرد. چنین حمله‌ای دارای پتانسیل شدیدی است، شبیه آسیب پذیری EternalBlue که پیش از این برای گسترش بدافزار WannaCry مورد استفاده قرار گرفته بود.

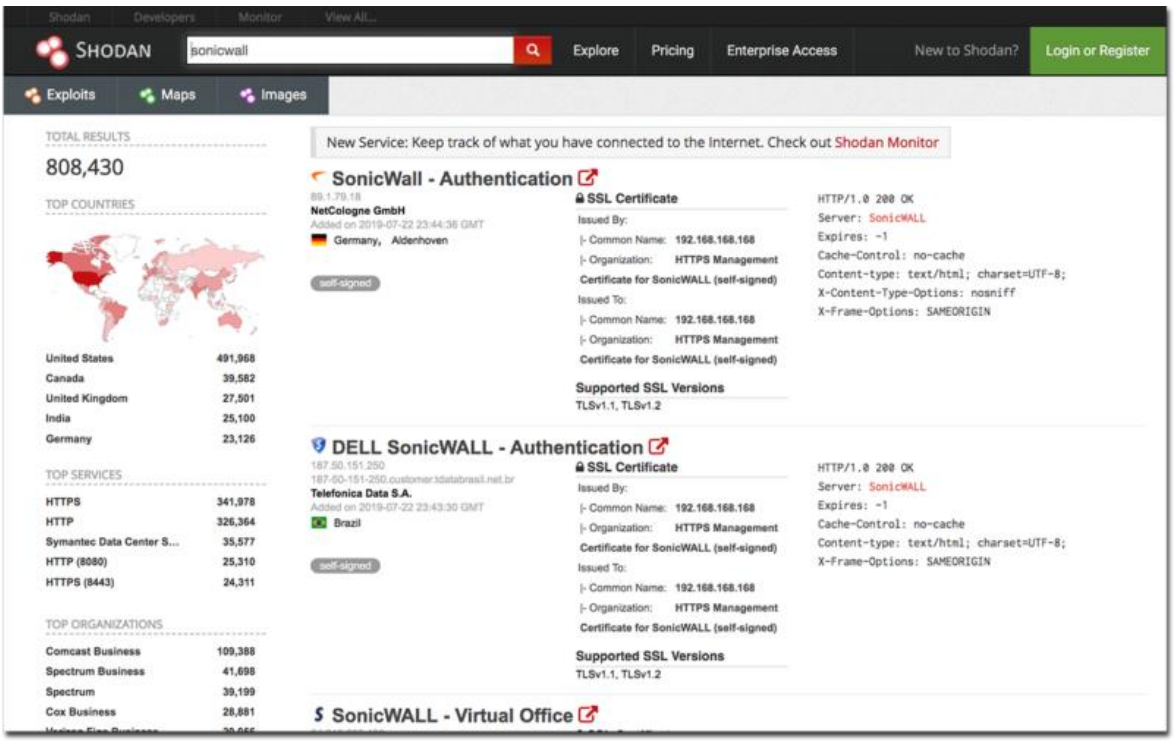
۱-۴ سناریو اول: حمله به تجهیزات دفاعی شبکه



تصویر ۱: نمایی از سناریوی حمله به تجهیزات دفاعی شبکه

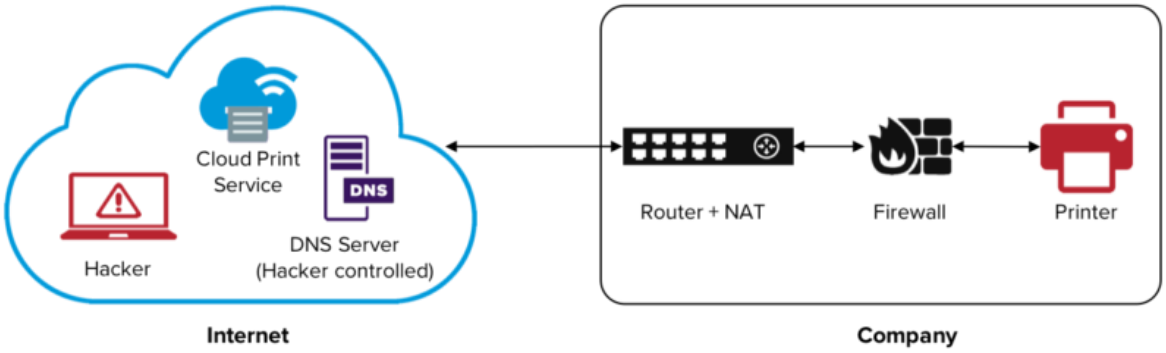
اولین سناریوی حمله بر دستگاه‌های VxWorks مستقر در محیط شبکه مانند فایروال‌ها تأثیر می‌گذارد. این دستگاه‌ها در معرض حملات مستقیمی از اینترنت هستند و به گونه‌ای طراحی شده اند که بسیار ایمن باشند؛ زیرا تمام شبکه داخلی که از آن محافظت می‌کنند، به آنها بستگی دارد. با استفاده از آسیب‌پذیری‌های URGENT/11، یک مهاجم می‌تواند یک حمله کامل بر روی این دستگاه‌ها و متعاقباً بر روی شبکه‌هایی که از آنها محافظت می‌کنند، انجام دهد.

به عنوان نمونه ای از این سناریو، در نظر بگیرید که چگونه چنین حمله‌ای می‌تواند دیوار آتش SonicWall را که روی سیستم عامل تحت تأثیر VxWorks اجرا می‌شود، تصاحب کند. طبق یافته‌های Shodan، بیش از ۸۰۸ هزار فایروال SonicWall به اینترنت متصل شده اند و در نتیجه تعداد مشابهی از شبکه‌هایی که این دستگاه‌ها از آن‌ها دفاع می‌کنند، وجود دارد. با استفاده از URGENT/11 و اتصال به اینترنت، یک مهاجم می‌تواند یک حمله مستقیم را با یک بسته TCP دستکاری شده خاص انجام دهد و تمام فایروال‌ها را به طور همزمان کنترل کرده و یک botnet را در اندازه‌ای تقریباً بی نظیر ایجاد کند که تمام شبکه‌های پشت سر آن-ها را به دست بگیرد.



تصویر ۲: نتیجه سایت sohdan برای فایروال‌های sonicwall مورد استفاده

۲-۴ سناریو دوم: حمله از خارج از شبکه با دور زدن امنیت



تصویر ۳: نمایی از سناریوی حمله خارج از شبکه

سناریوی حمله دوم بر روی هر دستگاه VxWorks که دارای اتصال به شبکه خارجی است، تأثیر می‌گذارد. آسیب‌پذیری‌های URGENT/11 مهاجمان را قادر می‌سازد بدون در نظر گرفتن هرگونه فایروال یا راه حل‌های NAT که در حاشیه شبکه برای جلوگیری از حملات اجرا می‌شوند، کنترل چنین دستگاه‌هایی را به دست آورند. ماهیت سطح پایین آسیب‌پذیری‌ها باعث می‌شود که این حمله در ارزیابی‌های امنیتی مشهود نباشد؛ زیرا به عنوان ارتباطات شبکه‌ای خوش‌خیم تلقی می‌شود.

به عنوان نمونه‌ای از این سناریو، یک حمله به دستگاه IoT متصل به ابر از یک شبکه مطمئن - مانند چاپگر Xerox را در نظر بگیرید. این چاپگر مستقیماً در معرض اینترنت قرار نمی‌گیرد، زیرا هم از طریق فایروال و هم با راه حل‌های NAT محافظت می‌شود و از طریق آن به یک برنامه ابری متصل می‌گردد (مانند Google Cloud Printing در این مورد). یک مهاجم می‌تواند اتصال TCP چاپگر به ابر را (بدون در نظر گرفتن TLS) رهگیری کند و با کنترل کامل بر آن، یکی از آسیب پذیری‌های کنترل کد از راه دور URGENT/11 را بر روی پرینتر اجرا کند. برای متوقف کردن اتصال TCP، یک مهاجم می‌تواند از تکنیک هایی مشابه روش‌های مورد استفاده توسط بدافزار DNSpionage استفاده کند، که سرورهای DNS را هدف قرار داده و به عنوان مرد میانی (MITM) در ترافیک اینترنت سازمان قرار می‌گرفت. هنگامی‌که مهاجم کنترل یک دستگاه را در شبکه به دست گرفت، می‌تواند گسترش یافته و کنترل سایر دستگاه‌های VxWorks شبکه را نیز به دست آورد.

۳-۴ سناریو سوم: حمله از درون شبکه

در این سناریو، یک مهاجم که قبلاً در نتیجه یک حمله قبلی در داخل شبکه قرار گرفته است، مانند سناریوهایی که قبلا توضیح داده شد، می‌تواند به دستگاه‌های VxWorks هدف، بسته‌هایی با قابلیت کنترل کامل دستگاه، ارسال کند، بدون اینکه تعامل کاربر لازم باشد. علاوه بر این، حمله‌کننده نیازی به اطلاعات قبلی در مورد دستگاه‌های هدف ندارد، زیرا URGENT/11 به او اجازه می‌دهد تا با پخش بسته‌های مخرب خود در سراسر شبکه، همه دستگاه‌های آسیب‌پذیر را به طور همزمان تحت تاثیر قرار دهد.

به عنوان نمونه‌ای از چنین حمله ای، دستگاهی مهم را در نظر بگیرید که فقط اتصالات شبکه داخلی داشته باشد، مانند دستگاه ناظر بیمار در یک بیمارستان. با وجود اینکه هیچ ارتباطی به اینترنت ندارد، یک نفوذ کننده به شبکه می‌تواند کنترل آن را به دست آورد. اگرچه ممکن است فکر کنید مخفی کردن یک دستگاه در داخل شبکه ایمن، ممکن است کافی باشد؛ اما همواره برای مهاجمان راهی وجود دارد که از آن به داخل شبکه وارد شوند، مانند سناریوهای قبلی که توضیح داده شد و جزئیات نحوه نفوذ به شبکه توسط مهاجم با استفاده از URGENT/11 را بیان می‌کرد.

نمونه دیگر را می‌توان در کنترل‌کننده‌های منطقی قابل برنامه‌ریزی (PLCها) یافت، که در کارخانه‌ها استفاده می‌شوند. از آنجا که آنها روی VxWorksهای آسیب‌پذیر اجرا می‌شوند، مهاجمی‌که از URGENT/11 استفاده کند، می‌تواند یک بار حمله‌ای را در شبکه پخش کرده و به طور موثق و بدون هیچ گونه تلاش برای شناسایی، کنترل کل کارخانه را در دست بگیرد، و آن را برای باج‌گیری یا هر هدف مخرب دیگری استفاده کند.

۵ مشخصه‌های آسیب پذیری

URGENT/11 شدیدترین آسیب پذیری‌های موجود در VxWorks تا به امروز است که در تاریخ ۳۲ ساله خود فقط از ۱۳ آسیب‌پذیری CVE عمومی‌رنج می‌برد. URGENT/11 یک گروه منحصر به فرد از آسیب-پذیری‌ها است که به مهاجمان اجازه می‌دهد تا NATها و فایروال‌ها را دور بزنند و کنترل راه دور دستگاه‌ها را از طریق پشته TCP / IP کشف نشده، بدون نیاز به تعامل کاربر به دست آورند. این به دلیل موقعیت سطح پایین آسیب‌پذیری‌ها در داخل پشته TCP/IP است که باعث می‌شود حملات به عنوان فعالیت مشروعی در شبکه تلقی شوند. چنین آسیب‌پذیری‌هایی با استفاده از پشته شبکه برای دستگاه‌های مختلف نیازی به سازگاری ندارند، و باعث می‌شود که توزیع آنها فوق العاده آسان باشد. در اکثر سیستم عامل‌ها، این آسیب پذیری‌های اساسی در پشته‌های شبکه، پس از سالها بررسی و کشف و جلوگیری از چنین نقص هایی، منقرض شده اند.

۵-۱ شش آسیب پذیری مهم با امکان اجرای کد از راه دور

URGENT / 11 مجموعه ۱۱ آسیب پذیری است که بر روی پشته TCP / IP (IPnet) که توسط نسخه‌های VxWorks استفاده می‌شود، تأثیر می‌گذارد. شش مورد از آسیب پذیری‌ها به عنوان مهم طبقه بندی شده اند و امکان اجرای کد از راه دور (RCE) را فراهم می‌کنند. این آسیب‌پذیری‌ها در ادامه شرح داده شده اند.

۵-۱-۱ سرریز پشته در تجزیه گزینه‌های IPv4 (CVE-2019-12256)

این آسیب پذیری می‌تواند توسط یک بسته IP خاص ساخته شده به دستگاه هدف ارسال شود، حتی به صورت چندپخشی[۲] یا همه‌پخشی[۳]. در این آسیب‌پذیری، نیازی به اجرای برنامه یا پیکربندی خاص روی دستگاه نیست و روی هر دستگاهی که VxWorks v6.9.4 یا بالاتر را با اتصال به شبکه اجرا کند، تأثیر می‌گذارد. این آسیب‌پذیری باعث سرریز پشته در استفاده از گزینه‌های IP در هدر IPv4 شده و دستیابی به RCE توسط آن آسان می‌شود.

[2] Multicast
[3] Broadcast

۵-۱-۲ چهار آسیب پذیری فساد حافظه ناشی از کنترل اشتباه قسمت نشانگر فوری[۴] TCP (CVE-2019-12255، CVE-2019-12260، CVE-2019-12261، CVE-2019-12263)

آسیب پذیری‌های یاد شده همه ناشی از استفاده نادرست از قسمت نشانگر فوری TCP است. این یک قسمت محرمانه TCP است که به ندرت در برنامه‌های مدرن استفاده می‌شود. یک مهاجم می‌تواند با اتصال مستقیم به یک پورت TCP باز در دستگاه مورد نظر یا با ربودن یک اتصال TCP برون‌مرزی که از دستگاه هدف گرفته شده است، از عملکرد اشتباه این قسمت، سوءاستفاده کند. پس از آن، این آسیب پذیری‌ها باعث می‌شود برنامه مورد نظر در دستگاه هدف بایت‌های بیشتری را از آنچه انتظار می‌رود از عملکرد recv() سیستم دریافت شده باشد، دریافت کند و منجر به اختلال حافظه در پشته، heap یا متغیرهای بخش داده سراسری شود - بسته به این که کدام بافر به تابع recv() منتقل شده است. این بدان معناست که یک مهاجم می‌تواند اتصالات مختلف TCP دستگاه مورد نظر (یا ورودی یا برون مرزی) را مورد بررسی قرار داده و به برنامه ای با ساده‌ترین بهره‌برداری، حمله کند.

از آنجا که قسمت نشانگر فوری یک ویژگی داخلی TCP است، روترها، NATها و حتی فایروال هایی که بین دستگاه هدف و حمله کننده قرار دارند، احتمالاً آن را به صورت دست نخورده منتقل می‌کنند. این بدان معناست که حتی یک اتصال TCP که از یک دستگاه آسیب پذیر به اینترنت از طریق چندین روتر، NAT و فایروال منتقل می‌شود، باز هم می‌تواند توسط یک مهاجم در اینترنت ربوده شده و از آن برای بهره‌برداری از آسیب‌پذیری استفاده شود. این امکان می‌تواند یک مهاجم را قادر سازد نه تنها دستگاه‌های آسیب‌پذیر که در غیر این حالت در شبکه‌های داخلی ایمن هستند، به تصرف خود درآورد، بلکه از طریق این مسیر به شبکه آن‌ها نیز نفوذ کند.

۵-۱-۳ سرریز Heap در تجزیه و تحلیل پیشنهاد DHCP / ACK در ipdhcpc (CVE-2019-12257)

این آسیب پذیری، یک مشکل سرریز پشته‌ای است که وقتی یک دستگاه آسیب پذیر، بسته‌های پاسخی ویژه DHCP دستکاری شده را می‌سازد، ایجاد می‌شود. این بسته‌ها توسط کاربر داخلی DHCP در VxWorks، ipdhcpc، تجزیه و تحلیل می‌شوند، هنگامی‌که این قسمت تلاش می‌کند تا آدرس IP را از یک سرور DHCP به دست آورد. مهاجمی‌که در همان زیر شبکه هدف قرار دارد، می‌تواند منتظر هدف بماند تا درخواست DHCP را ارسال کند، و سریعا با پاسخ DHCP ویژه ساختگی پاسخ دهد. در این سناریو، دستگاه مورد نظر

[4] Urgent Pointer

منتظر پاسخ از سرور اصلی DHCP شبکه خواهد بود که توسط مهاجم به راحتی فریب داده می‌شود و پیام پاسخ دستکاری شده DHCP را تجزیه می‌کند. این امر منجر به سرریز Heap با داده‌های کنترل شده توسط مهاجم می‌شود که می‌تواند منجر به اجرای کد از راه دور شود. این آسیب پذیری روی نسخه‌های VxWorks از ۶.۵ تا ۶.۹.۳ اثر می‌گذارد.

۵-۲ پنج آسیب پذیری انکار سرویس، نشت اطلاعات یا نقص‌های منطقی

آسیب پذیری‌های باقی مانده به عنوان انکار سرویس، نشت اطلاعات یا نقص منطقی طبقه بندی می‌شوند. از آنجا که هر آسیب پذیری روی بخش دیگری از پشته شبکه تأثیر می‌گذارد، بر مجموعه دیگری از نسخه‌های VxWorks تأثیرگذار است. به عنوان یک گروه، URGENT/11 روی هرکدام از نسخه‌های VxWorks تحت تاثیر، حداقل یک آسیب پذیری RCE وجود دارد. طیف گسترده‌ای از نسخه‌های تحت تأثیر در طی ۱۳ سال گذشته یک اتفاق نادر در عرصه سایبری است و در نتیجه‌ی ابهام نسبی VxWorks در جامعه پژوهشی به وجود آمده است. این مدت زمان ممکن است حتی طولانی‌تر باشد، زیرا طبق گفته Wind River، سه مورد از آسیب پذیری‌ها در IPnet از زمانی وجود داشتند که این پشته را در سال ۲۰۰۶ از Interpeak بدست آورده است.

۵-۲-۱ انکار سرویس روی اتصال TCP از طریق گزینه‌های TCP نامناسب (CVE-2019-12258)

این آسیب پذیری روی نسخه‌های ۶.۵ و بالاتر VxWorks تأثیر می‌گذارد و اجازه می‌دهد از هر اتصال TCP حملات انکار سرویس به دستگاه‌های VxWorks تحت تاثیر یا از آن‌ها شکل گیرند.

۵-۲-۲ رسیدگی به پاسخ‌های ARP معکوس ناخواسته (نقص منطقی) (CVE-2019-12262)

این آسیب پذیری یک خطای منطقی است که روی نسخه‌های ۶.۵ و بالاتر VxWorks تأثیر می‌گذارد و می‌تواند به یک مهاجم در همان زیر شبکه اجازه دهد چندین آدرس IPv4 را از طریق بسته‌های پاسخی RARP ناخواسته به دستگاه مورد نظر اضافه کند. این امر جداول مسیریابی دستگاه مورد نظر را مختل کرده و می‌تواند منجر به حمله DoS روی هر برنامه TCP / IP مورد استفاده شود. چندین بار استفاده از این آسیب پذیری نیز می‌تواند باعث خستگی حافظه شده و منجر به اختلال اجرایی اضافی در دستگاه هدف شود.

۵-۲-۳ عیب منطقی در تعیین IPv4 توسط کاربر ipdhcpc DHCP (CVE-2019-12264)

این آسیب پذیری یک خطای منطقی در سرویس گیرنده DHCP VxWorks است، (ipdhcpc) که روی نسخه‌های ۶.۵ و بالاتر VxWorks تأثیر می‌گذارد. یک دستگاه آسیب‌پذیر هر آدرس IPv4 را که توسط یک

سرور DHCP به آن اختصاص داده شده است، می‌پذیرد، حتی اگر این آدرس یک آدرس تک‌پخشی[5] غیر معتبر باشد (چندپخشی، همه‌پخشی یا سایر آدرس‌های غیرقانونی). مشابه آسیب پذیری RARP که در بالا به آن اشاره شد، یک مهاجم در همان زیر شبکه می‌تواند دستگاه هدف را مجبور به انتصاب آدرس‌های IP غیرمعتبر کند که این امر منجر به جداول مسیریابی نادرست و مختل شدن اتصال شبکه دستگاه مورد نظر خواهد شد. علاوه بر این، اختصاص یک آدرس IP چندپخشی به دستگاه هدف، دستگاه را نیز در برابر آسیب پذیری‌های مربوط به IGMP که در ادامه شرح داده شده، قابل بهره‌برداری می‌کند.

۵-۲-۴ DoS از طریق NreLreferance در تجزیه IGMP (CVE-2019-12259)

این آسیب‌پذیری، از نوع انکار سرویس است که روی نسخه‌های ۶.۵ و بالاتر VxWorks تأثیر می‌گذارد و می‌تواند از طریق یک بسته غیرمجاز ارسال شده از مهاجمان در زیر شبکه محلی منجر به نفوذ به یک وسیله هدف شود. برای ایجاد این آسیب پذیری، یک مهاجم ابتدا از طریق یک بسته پاسخی ویژه DHCP، دستگاه هدف را وادار به انتصاب یک آدرس چندپخشی می‌کند. سپس مهاجم می‌تواند یک بسته پرس و جو عضویت IGMPv3 را به دستگاه مورد نظر ارسال کند و منجر به ایجاد NULL در پشته شبکه و خرابی دستگاه مورد نظر شود.

۵-۲-۵ نشت اطلاعات IGMP از طریق گزارش عضویت خاص IGMPv3 (CVE-2019-12265)

این آسیب پذیری یک نشت اطلاعات است که روی نسخه‌های ۶.۹.۳ و بالاتر از VxWorks تأثیر می‌گذارد. یک دستگاه در صورت داشتن آدرس چندپخشی که به رابط شبکه آن تخصیص داده شده، تحت تأثیر این آسیب پذیری قرار می‌گیرد که می‌توان از طریق آسیب پذیری کاربر DHCP که قبلا توضیح داده شد (CVE-2019-12264) به این مورد رسید. برای ایجاد این آسیب پذیری، یک مهاجم می‌تواند یک گزارش پرس و جو از عضویت IGMPv3 را که روی چند قطعه[6] IP بسته‌بندی شده است به دستگاه مورد نظر ارسال کند. این امر منجر به نشت اطلاعات از بسته‌های مورد نظر از طریق گزارش عضویت IGMPv3 می‌گردد که به مهاجم ارسال می‌شود.

[5] Unicast
[6] Fragment

۶ اقدامات جهت کاهش شدت آسیب پذیری

سازمان‌ها و سازندگان دستگاه هایی که دستگاه‌های VxWorks را استفاده می‌کنند باید فوراً دستگاه‌های آسیب دیده را وصله کنند. اطلاعات بروزرسانی و وصله را می‌توان در هشدار امنیتی Wind River که در آدرس زیر قرار گرفته، یافت:

https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

۷ جمع بندی و نتیجه‌گیری

طی دو ماه اخیر تیم تحقیقاتی آرمیس از آسیب‌پذیری‌های Wind River، شرکتی که VxWorks را ساخته و نگهداری می‌کند، پرده برداشت و با آنها در زمینه توسعه راه‌حل‌ها و ساخت وصله‌ها و همچنین آگاه ساختن سازندگان دستگاه‌های آسیب‌دیده همکاری کرده است. آسیب‌پذیری‌های URGENT/11 توزیع‌های NoteVxWorks تا نسخه ۶.۵ را تحت تأثیر می‌گذارد، اما نسخه‌های طراحی شده برای صدور گواهینامه ایمنی - VxWorks 653 و VxWorks Cert Edition، که توسط صنایع زیرساختی منتخب مانند حمل و نقل استفاده می‌شوند، تحت تاثیر نیستند.

URGENT/11 ممکن است دسترسی گسترده تری داشته باشد زیرا IPnet قبل از دستیابی آن توسط VxWorks در سال ۲۰۰۶، در سیستم‌عامل‌های‌دیگر نیز مورد استفاده قرار گرفت. با این حال، در این باره اطلاعاتی در دست نیست. آسیب پذیری‌های URGENT/11 تخمین زده می‌شود دستگاه‌هایی مانند سیستم-های SCADA، کنترلرهای آسانسور و صنعتی، مانیتور بیمار و دستگاه‌های MRI و همچنین فایروال‌ها، روترها، مودم‌ها، تلفن‌های VOIP و چاپگرها را تحت تاثیر قرار دهد. به سازندگان دستگاه‌هایی که VxWorks را اجرا می‌کنند، توصیه می‌شود آخرین نسخه‌های هشدار امنیتی Wind River را که در مرکز امنیت شرکت ارسال شده است، بررسی کنند و سریعاً آنها وصله نمایند.

Wind River در بیانیه ای گفت: "همه آسیب پذیری‌ها در مورد تمام نسخه‌های آسیب دیده پیدا نمی‌شوند. تا امروز هیچ کدام از آسیب پذیری‌های Urgent / 11 در حملات استفاده نشده است. دستگاه‌های تحت تأثیر، زیر مجموعه کوچکی از مشتری‌های ما را تشکیل می‌دهند و در درجه اول شامل دستگاه‌های سازمانی واقع در حاشیه شبکه‌های سازمانی هستند که با اینترنت در ارتباطند، مانند مودم، روتر و پرینتر و همچنین برخی از دستگاههای صنعتی و پزشکی. دستگاههای دارای VxWorks باید دستگاههای آسیب دیده را بلافاصله وصله کنند. "

۸ منابع

[1] https://www.wired.com/story/vxworks-vulnerabilities-urgent11/

[2] https://www.armis.com/urgent11/

[3] https://www.zdnet.com/article/urgent11-security-flaws-impact-routers-printers-scada-and-many-iot-devices/