سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی یک آسیب‌پذیری بحرانی در مودم‌های کابلی

اسفند ۹۸

۱ چکیده

اخیرا محققان یک آسیب‌پذیری بحرانی در مودم‌های کابلی پیدا کرده‌اند که ممکن است صدها میلیون مودم را در سراسر جهان تحت تاثیر قرار دهد. این آسیب‌پذیری مربوط به سیستم‌های روی یک تراشه[۱] Broadcom است که در بسیاری از مودم‌های کابلی مورد استفاده قرار می‌گیرد، به ویژه در نرم‌افزارهایی برای مقاومت در برابر افزایش قدرت سیگنال، تحلیلگر spectrum را اجرا می‌کنند. در ادامه به بررسی بیشتر این آسیب‌پذیری خواهیم پرداخت.

۲ محصولات تحت تاثیر

تمامی مودم‌هایی که دارای تراشه مجتمع Broadcast هستند، در برابر این نقص نرم‌افزاری، آسیب‌پذیرند. محققان پیش‌بینی کرده‌اند که این آسیب‌پذیری، صدها میلیون مودم کابلی را تحت تاثیر قرار می‌دهد.

۳ تاثیر آسیب‌پذیری

بهره‌برداری از این آسیب‌پذیری، نیازمند دسترسی به شبکه محلی مودم است، اما مهاجمان ماهر می‌توانند کد مربوط به حمله را در صفحات وب یا پیام‌های الکترونیکی قرار دهند. به این طریق، وقتی کاربران این صفحات وب را در مرورگر باز کنند، آلوده خواهند شد.

به گفته محققان، مهاجمان موفق می‌توانند با بهره‌برداری از این آسیب‌پذیری، کنترل مودم را به دست گیرند و کاربران شبکه هک شده را به وب‌سایت‌های مخرب انتقال دهند، حملات مردی در میان روی تراکنش‌ها انجام دهند و یا firmware مودم را تغییر دهند.

۴ مشخصه‌های آسیب‌پذیری

شناسه CVE-2019-19494 به این آسیب‌پذیری اختصاص داده شده است. گفته شده حدود ۲۰۰ میلیون مودم آسیب‌پذیر، فقط در اروپا وجود دارد و تاکنون از بین مودم‌های تست شده، دستگاهی نبوده که بدون بروز کردن firmware، در برابر این آسیب‌پذیری مقاوم بوده باشد و از این رو، نمی‌توان تخمین دقیقی از گستره این آسیب‌پذیری به دست آورد.

[۱] System on a chip

۴-۱ جزییات آسیب‌پذیری

آسیب‌پذیری مورد بحث که با نام Cable Haunt شناخته می‌شود، در دو مرحله مورد بهره‌برداری قرار می‌گیرد. ابتدا دسترسی به نقطه انتهایی آسیب‌پذیر از طریق یک کاربر در شبکه محلی مانند مرورگر بدست می‌آید. سپس، نقطه انتهایی آسیب‌پذیر با حمله سرریز بافر مورد هدف قرار می‌گیرد که به مهاجم امکان کنترل مودم را می‌دهد.

۴-۱-۱ دسترسی به نقطه انتهایی

نقطه پایانی که به ابزاری به نام تحلیلگر Spectrum خدمت می‌کند، از یک WebSocket برای ارتباط با پیش زمینه گرافیکی نمایش داده شده در مرورگر استفاده می‌کند. با این که CORS[۲] دسترسی به چنین نقطه پایانی را برای درخواست HTTP محدود می‌کند، اما WebSocket توسط این پروتکل محافظت نمی‌شود. بنابراین، سرور این وظیفه را دارد که پارامترهای درخواست مربوطه را که توسط مرورگر اضافه شده، تأیید کند. از آنجا که این پارامترها هرگز توسط مودم کابلی مورد بررسی قرار نمی‌گیرند، WebSocket درخواست‌های ساخته شده توسط جاوا اسکریپت را که بدون در نظر گرفتن مبدأ در مرورگر اجرا می‌شوند، می‌پذیرد و از این طریق به مهاجمان اجازه می‌دهد تا به نقطه انتهایی برسند. لازم به ذکر است که بهره‌برداری محدود به اجرا در یک مرورگر نیست. هر جایی که در آن، با اجرای کد در آن بتوان به یک آدرس IP در شبکه محلی رسید، می‌تواند برای بهره برداری از Cable Haunt استفاده شود.

۴-۱-۲ تحت کنترل درآوردن

پس از رسیدن به WebSocket ، آسیب‌پذیری سرریز بافر قابل بهره برداری است. درخواست‌های WebSocket به صورت JSON ارائه می‌شوند. تجزیه‌گری که این درخواست JSON را تفسیر می‌کند، بدون در نظر گرفتن طول، پارامترهای ورودی را در بافر کپی می‌کند و اجازه می‌دهد مقادیر موجود در پشته رونویسی شوند. در میان این مقادیر، ثبات‌های ذخیره شده مانند شمارنده برنامه و آدرس برگشتی ذخیره می‌شوند. با یک پیامی که به دقت ساخته شده، می‌توان مودم را طوری دستکاری کرد که کد دلخواه مشخص شده توسط مهاجمی از راه دور را اجرا کند. پس از به دست گرفتن کنترل توسط مهاجم، از بسیاری جهات می توان از این آسیب‌پذیری سوءاستفاده کرد. برخی از نمونه‌ها عبارتند از:

- تغییر سرور DNS پیش‌فرض
- انجام حملات مردی در میان از راه دور

[۲] HTTP access control

- تعویض کد یا حتی کل firmware
- بارگذاری، پاک کردن و یا بروزرسانی firmware
- غیرفعال کردن بروزرسانی firmware
- تغییر هر فایل پیکربندی یا تنظیمات
- به دست آوردن و تنظیم مقادیر OID
- تغییر همه آدرس‌های MAC مرتبط
- تغییر شماره سریال‌ها
- استفاده از دستگاه در یک بات‌نت

۵ اقدامات جهت کاهش شدت آسیب‌پذیری

برای مقابله با اثرات سوء ناشی از این آسیب‌پذیری، تولیدکننده دستگاه شما وصله این آسیب‌پذیری را منتشر کرده است یا نه. در صورت انتشار وصله‌های مربوطه، firmware دستگاه خود را بروزرسانی نمایید.

۶ جمع بندی و نتیجه‌گیری

اخیراً محققان یک آسیب‌پذیری بحرانی در مودم‌های کابلی کشف کرده‌اند که پیش‌بینی می‌شود صدها میلیون مودم در سراسر جهان را تحت تاثیر قرار می‌دهد. این آسیب‌پذیری با نام cable haunt شناخته می‌شود. یک مهاجم، با بهره‌برداری از این آسیب‌پذیری می‌تواند کنترل دستگاه را به دست آورده و اقدامات مخربی روی آن انجام دهد. برای مقابله با این نقص نرم‌افزاری، لازم است firmware مودم‌ها به آخرین نسخه منتشر شده که در آن آسیب‌پذیری cable haunt وصله شده، بروزرسانی شود.

۷ منابع

[1] https://cablehaunt.com

[2] https://www.tomsguide.com/news/cable-haunt-modem-flaw