آسیب‌پذیری man-in-the-middle در بستر ارتباطی

فهرست مطالب

1 مقدمه

CWMP مخفف CPE WAN Management Protocol می‌باشد که یک پروتکل برای ارتباط بین تجهیزات سمت مشتری (CPE)[1] و سرویس‌دهنده پیکربندی خودکار (ACS)[2] است. این پروتکل مکانیزمی را تعریف می‌کند که شامل پیکربندی خودکار امن برای تجهیزات سمت مشتری می‌شود و همچنین سایر توابع مدیریت CPE را به یک چارچوب مشترک تبدیل می‌کند.

2 آسیب‌پذیری man-in-the-middle در بستر ارتباطی

به دلیل اینکه بسیاری از ISPها ارتباط بین ACS و تجهیزات مشتری را رمزنگاری نمی‌کنند و دسترسی به آدرس IP یا MAC را محدود نمی‌کنند؛ در نتیجه شرایط برای حمله "man-in-the-middle" آسان است. با توجه به آسیب‌پذیر بودن CWMP، مهاجم می‌تواند عملاً هر کاری مانند تنظیم و خواندن پارامترهای پیکربندی، تنظیم مجدد پارامترها به مقادیر پیش‌فرض آن و راه‌اندازی مجدد دستگاه را از راه دور انجام دهد. شایع‌ترین نوع حمله این است که آدرس‌های DNS را در تنظیمات روتر برای آدرس‌های سرورهای تحت کنترل مهاجم جایگزین کنند. آنها درخواست‌های وب را فیلتر کرده و کسانی را که به خدمات بانکی مراجعه کردند به صفحات جعلی هدایت می‌کنند. صفحات جعلی برای همه سیستم‌های پرداخت عمومی مانند PayPal، Visa، MasterCard، QIWI و دیگر موارد ایجاد شده‌اند.

3 محصولات تحت تأثیر آسیب‌پذیری

علاوه بر روترها، این آسیب‌پذیری بر تلفن‌های VoIP، دوربین‌های شبکه و سایر تجهیزاتی که این امکان را فراهم می‌آورند تا پیکربندی از راه دور از طریق CWMP انجام شود، تأثیر می‌گذارد.

4 اقدامات جهت مقابله با آسیب‌پذیری

- از دیواره آتش جهت مسدود کردن تمام اتصالات به پورت TCP 7547، به جز از IPهای قابل اعتماد استفاده کنید.
- اگر از تنظیمات خودکار ACS استفاده نمی‌کنید، آن را غیرفعال کنید که آسان‌ترین و مؤثرترین راه‌حل است.

[1] Customer-Premises Equipment
[2] Auto-Configuration Server