باسمه تعالی

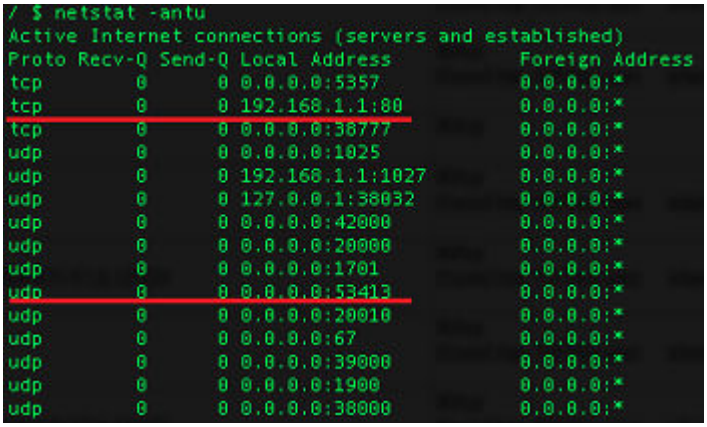
وجود راه ورود مخفی در مسیریاب‌های Netcore

(Netis)

شرح آسیب‌پذیری

در شهریور ماه سال ۱۳۹۴ مشخص شد که مسیریاب‌های شرکت Netcore (که برندی محبوب برای تجهزات شبکه در کشور چین است) دارای یک راه ورود مخفی (backdoor) خطرناک هستند که به سادگی می‌تواند مورد سوءاستفاده‌ی حمله‌کنندگان قرار گیرد. این محصولات در بیرون از چین تحت نام Netis فروخته می‌شوند. این راه ورود مخفی امکان اجرای کدهای دلخواه را برای تبهکاران سایبری فراهم می‌سازد.

این راه ورود مخفی در واقع یک پورت باز UDP با شماره پورت 53413 می‌باشد که از سمت WAN در مسیریاب قابل دسترسی است. این بدان معناست که اگر مسیریاب دارای یک آدرس IP قابل دسترس از خارج باشد، حمله‌کننده می‌تواند از هرجا به این backdoor متصل شود.



خروجی دستور Netstat توسط ادمین (پورت backdoor هایلایت شده است)

راه ورود مخفی توسط یک کلمه عبورِ تعبیه شده در میان‌افزارِ مسیریاب مراقبت می‌شود. همه مسیریاب‌های Netcore/Netis از پسورد مشابهی استفاده می‌کنند. این مراقبت در عمل بی تاثیر است، چرا که حمله‌گر می‌تواند به راحتی به این مسیریاب login کند و کاربران نمی‌توانند این رخنه را غیرفعال کرده یا تغییر دهند.

طبق اطلاعات گردآوری شده، تمامی مسیریاب‌های Netcore/Netis دارای این آسیب‌پذیری هستند. در پویش انجام گرفته توسط محققان امنیتی، بیش از دو میلیون آدرس IP با این پورت بازِ UDP پیدا شده است. تقریباً

تمامی این مسیریاب‌ها در کشور چین قرار دارند. تعداد کمتری از آن‌ها نیز در کشورهایی مانند کره جنوبی، تایوان، اسرائیل و آمریکا قرار دارند. در کشور ایران نیز مواردی از استفاده از این محصول مشاهده شده است.

حمله‌گر علاوه بر login، می‌تواند فایل‌های دلخواه خود را در مسیریاب آپلود، دانلود و اجرا کند. این امر موجب می‌شود تا حمله‌گر کنترلِ تقریباً کاملی بر روی مسیریاب داشته باشد. برای مثال، وی می‌تواند مسیریاب را به‌گونه‌ای تنظیم کند که حمله‌ی فردی در میان (man-in-the-middle) شکل گیرد. به‌علاوه حمله‌گر می‌تواند فایلِ حاوی نام کاربری و کلمه عبور مربوط به پنل مسیریاب را (که به صورت رمز نشده در مسیریاب ذخیره شده) دانلود کند (شکل زیر).

```
In [139]: n.dogetpasswd()
web_user_info=1
array_index=0;;comm.flags=1;;comm.id=0;;user=guest;;password=guest;;user_type=1;;
web_user_info=1
```

به منظور تشخیص آسیب‌پذیری یک مسیریاب، می‌توان از یک پویشگر پورت آنلاین استفاده کرد. در این صورت نتیجه پویش پورت 53413 مشابه شکل زیر خواهد بود (به قسمتی از عکس که زیر آن خط کشیده شده توجه شود).

پویش پورت UDP

برای حل این آسیب‌پذیری، راه‌حل‌های محدودی در اختیار کاربران قرار دارد. میان‌افزارهای متن‌بازی مانند dd-wrt و یا Tomato به ندرت مسیریاب‌های Netcore را پشتیبانی می‌کنند (به نظر می‌رسد تنها یکی از مسیریاب‌های آسیب‌پذیر توسط این دو میان‌افزار پشتیبانی می‌شود). به نظر می‌رسد بهترین راه چاره، جایگزین کردن این مسیریاب‌ها باشد.