

باسمه تعالی

وجود راه ورود مخفی در مسیر یاب‌های Netcore (Netis)

شرح آسیب پذیری

در شهریور ماه سال ۱۳۹۴ مشخص شد که مسیر یاب‌های شرکت Netcore (که برندی محبوب برای تجهیزات 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 مسیر یاب قابل دسترسی است. این بدان معناست که اگر مسیر یاب دارای یک آدرس IP قابل دسترسی از خارج باشد، حمله‌کننده می‌تواند از هر جا به این backdoor متصل شود.

```

/ $ netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5357            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.1:80         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:38777         0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:1025          0.0.0.0:*               LISTEN
udp        0      0 192.168.1.1:1027     0.0.0.0:*               LISTEN
udp        0      0 127.0.0.1:38032      0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:42000        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:20000        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:1701         0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:53413        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:20010        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:67           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:39000        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:1900         0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:38000        0.0.0.0:*               LISTEN

```

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

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

طبق اطلاعات گردآوری شده، تمامی مسیر یاب‌های Netcore/Netis دارای این آسیب پذیری هستند. در پوشش انجام گرفته توسط محققان امنیتی، بیش از دو میلیون آدرس IP با این پورت باز UDP پیدا شده است. تقریباً

تمامی این مسیرها 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 مسیر آپلود، دانلود و اجرا کند. این امر موجب می‌شود تا حمله‌گر کنترل تقریباً کاملی بر روی مسیر داشته باشد. برای مثال، وی می‌تواند مسیر را به‌گونه‌ای تنظیم کند که حمله‌ی فردی در میان (man-in-the-middle) شکل گیرد. به‌علاوه حمله‌گر می‌تواند فایل حاوی نام کاربری و کلمه عبور مربوط به پنل مسیر را (که به صورت رمز نشده در مسیر 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 مسیر، می‌توان از یک پوشگر پورت آنلاین استفاده کرد. در این صورت نتیجه پوش پورت 53413 مشابه شکل زیر خواهد بود (به قسمتی از عکس که زیر آن خط کشیده شده توجه شود).

```
Starting job... [2014-08-13 06:11:29] Stay on this page for results!

Starting Nmap 6.00 ( http://nmap.org ) at 2014-08-13 09:11 EEST
NSE: Loaded 17 scripts for scanning.
Initiating UDP Scan at 09:11
Scanning [redacted] [1 port]
Completed UDP Scan at 09:11, 0.15s elapsed (1 total ports)
Initiating Service scan at 09:11
Scanning 1 service on [redacted]
Discovered open port 53413/udp on [redacted]
Discovered open|filtered port 53413/udp on [redacted] is actually open
Completed Service scan at 09:12, 52.90s elapsed (1 service on 1 host)
NSE: Script scanning [redacted]

Nmap scan report for [redacted]
Host is up.

PORT STATE SERVICE VERSION
53413/udp open xdmcp XDMCP (unwilling; status: .Login;)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 68.77 seconds
Raw packets sent: 1 (28B) | Rcvd: 0 (0B)
```

پوش پورت UDP

برای حل این آسیب پذیری، راه حل های محدودی در اختیار کاربران قرار دارد. میان افزارهای متن بازی مانند dd-wrt و یا Tomato به ندرت مسیر یاب های Netcore را پشتیبانی می کنند (به نظر می رسد تنها یکی از مسیر یاب های آسیب پذیر توسط این دو میان افزار پشتیبانی می شود). به نظر می رسد بهترین راه چاره، جایگزین کردن این مسیر یاب ها باشد.