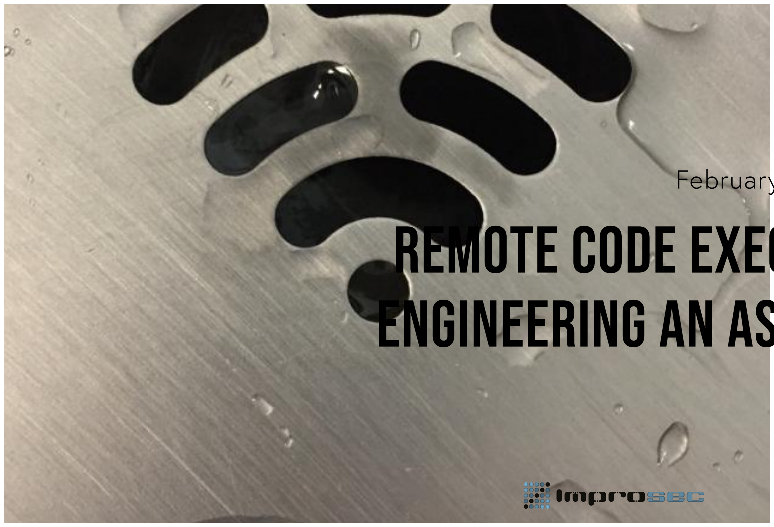


February 12, 2020

REMOTE CODE EXECUTION BY REVERSE ENGINEERING AN ASKEY WIFI-EXTENDER

Anders Kusk (/tech-blog?author=5e21c687c8ae141b3ef5aa77)

This blog highlights bugs and observations found in the WiFi-extender Askey AP4000W during an Improsec “Nerd Day”. Found bugs are reported to the vendor according to our Responsible Disclosure Policy, but this time in close collaboration with TDC.

TIMELINE:

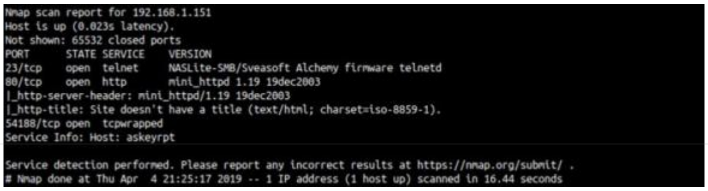
- The vulnerability and observations of firmware “AP4100W_TDC_V1.01.003” were disclosed to Askey on 17th of September 2019. No response received.
- The vulnerability and observations were disclosed to TDC on 27th of September 2019, as we knew they had customers running the product. TDC agreed to contact hardware vendor on behalf of Improsec, collaborate on getting it fixed, and getting customers updated.
- During December 2019 TDC tested a new firmware from Askey for these devices.
- Askey closed the insecure FTP-server 17th of December 2019, but we found it to be online again by 2nd of January 2020.
- TDC confirms that a new firmware has successfully been deployed to all available devices on 28th of January 2020.
- Insecure firmware FTP-server confirmed to have been secured on the 3rd of February 2020.

CVE REGISTERED:

- CVE: CVE-2020-8614 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8614)

PATH TO DISCOVERY

Connecting to and scanning the device with NMAP showed the following open ports.



```
Nmap scan report for 192.168.1.151
Host is up (0.023s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE    VERSION
23/tcp    open  telnet     NASLite-SMB/Sveasoft Alchemy firmware telnetd
80/tcp    open  http       mini_httpd 1.19 19dec2003
|_http-server-header: mini_httpd/1.19 19dec2003
|_http-title: Site doesn't have a title (text/html; charset=iso-8859-1).
54188/tcp open  tcpwrapped
Service Info: Host: askeyrpt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Apr  4 21:25:17 2019 -- 1 IP address (1 host up) scanned in 16.44 seconds
```

When doing an NMAP service scan, the service running on port 54188 crashed and a reboot was required to bring it back up. A telnet daemon was also seen on port 23, however, no valid passwords were found for the typical users(root/admin/busybox) in the documentation.

Viewing the circuit board showed no visible UART or JTAG interfaces, but reading