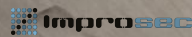


February 12, 2020

REMOTE CODE EXECUTION BY REVERSE ENGINEERING AN ASKEY WIFI-EXTENDER



powered by:
[Cookie Information \(https://cookieinformation.com/\)](https://cookieinformation.com/)

You control your data

We and our business partners use technologies, including cookies, to collect information about you for various purposes, including:

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

1. Functional
2. Statistical
3. Marketing

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. By clicking 'Accept', you give your consent for all these purposes. You can also choose to specify the purposes you consent to by ticking the checkbox next to the purpose and clicking 'Save settings'.

TIMELINE: You may withdraw your consent at any time by clicking the small icon at the bottom left corner of the website.

- The vulnerability and observations of firmware AP4000W, TDC V1.01.003" were disclosed to Askey on 17th of December 2019 and to TDC on 19th of December 2019. [Read more about cookies](#)
- 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. [Show details](#)
- 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 January 2020. [Strictly necessary](#) [Functional](#) [Statistical](#) [Marketing](#)
- 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           MSLSite-SMB/Sveasoft Alchemy firmware telnetd
88/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