SA-2021-02-01

Notification Date: February 24, 2021

SECURITY ADVISORY

DNSpooq DNS Cache Poisoning Vulnerabilities

Summary

Advantech industrial cellular routers, firmware versions 6.2.7 and prior, are vulnerable to the DNS cache poisoning attack as recently discovered by the JSOF Research Lab. The routers are however not affected by the high-severity buffer overflow vulnerabilities, which are also included in that report.

Issue Description

The JSOF Research Lab discovered several security vulnerabilities in dnsmasq, a popular lightweight DNS server, which is also used in the firmware of Advantech industrial cellular routers.

The reported collection of vulnerabilities (called DNSpooq) is divided into two types of vulnerabilities:

- **DNS cache poisoning attacks** that could allow an attacker to spoof a DNS response and thus redirect communication made towards a specific domain.
- **Buffer overflow vulnerabilities** that could lead to remote code execution when dnsmasq is configured to use DNSSEC.

For more details please see the technical whitepaper.

The router firmware does not use DNSSEC so it is immune to the buffer overflow vulnerabilities. It is however not immune to the cache poisoning attack.

A malicious client could send a large amount of forged DNS responses, trying to guess the TXID and port numbers of a valid DNS query. If one such response matches, a fake DNS record gets inserted into the dnsmasq cache. Traffic towards that domain will thus be sent to a malicious IP address, which enables e.g. man-in-the-middle attacks.

Due to the discovered vulnerabilities the probability of success in such case is not negligible, yet still quite low. For example, one would need to send 291.000 forged responses in 2 seconds (100 Mbps) to have a 50% probability of success. The most vulnerable are thus deployments with untrusted clients connected to the LAN, such as WiFi hostspots, for example.

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661

Affected Products

Firmware versions 6.2.7 and prior are affected by the DNSpooq, however only by the lower-severity cache poisoning vulnerabilities as described in the table below.

CVE	Type	Severity (CVSS)	Firmware Affected
CVE-2020-25681	Buffer overflow	8.1 (high)	None
CVE-2020-25682	Buffer overflow	8.1 (high)	None
CVE-2020-25683	Buffer overflow	5.9 (medium)	None
CVE-2020-25687	Buffer overflow	5.9 (medium)	None
CVE-2020-25684	Cache poisoning	4 (medium)	6.2.7 and prior
CVE-2020-25685	Cache poisoning	4 (medium)	6.2.7 and prior
CVE-2020-25686	Cache poisoning	4 (medium)	6.2.7 and prior

Solution

The firmware version 6.2.8 (released in February 2021) includes dnsmasq 2.84, which addresses all the reported DNSpooq vulnerabilities.

As a further precaution we recommend deployment of remote monitoring tools that can detect various suspicious activities. For more details see the Remote Monitoring Application Note.

For public WiFi hostspots and similar deployments we also recommend limiting the bandwidth that can be used by a single user, either using the Quality of Service (QoS) controls or the Captive Portal Router App.

Revision History

2021-02-24 Advisory published

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661