Bern, 5/18/2021

Statement WLAN Fragattack

Mathy Vanhoef, researcher in Computer Security, has found some issues in the 802.11 WLAN implementation. These issues are dealt with under the term Fragattack.

Details: https://papers.mathyvanhoef.com/usenix2021.pdf

The attacks in general allow the attacker:

- the injection of L2 frames (depending on the attack vector) into an encrypted WLAN network,
- the filtering of some network data under certain conditions.

These attacks target vulnerability in the fragmentation feature. This affects operation in client and access point mode. WLAN without encryption (e.g., Public WiFi) are not affected by the Fragattack vulnerabilities because the compromised security function is not applied due to the lack of encryption.

The WLAN drivers of all NetModule routers are affected by Fragattack. Therefore, NetModule soon provides the following releases for all still supported routers in order to close the security gaps:

- 4.5.0.104
- 4.4.0.110
- 4.3.0.112

A software update is recommended for all NetModule devices with WLAN features.

The following CVEs are addressed with the updates:

- CVE-2020-24586 - Fragmentation cache not cleared on reconnection
- CVE-2020-24587 - Reassembling fragments encrypted under different keys
- CVE-2020-24588 - Accepting non-SPP A-MSDU frames, which leads to payload being parsed as an L2 frame under an A-MSDU bit toggling attack
- CVE-2020-26139 - Forwarding EAPOL from unauthenticated sender
- CVE-2020-26140 - Accepting plaintext data frames in protected networks
- CVE-2020-26141 - Not verifying TKIP MIC of fragmented frames
- CVE-2020-26142 - Processing fragmented frames as full frames
- CVE-2020-26143 - Accepting fragmented plaintext frames in protected networks
- CVE-2020-26144 - Always accepting unencrypted A-MSDU frames that start with RFC1042 header with EAPOL ethertype
- CVE-2020-26145 - Accepting plaintext broadcast fragments as full frames
- CVE-2020-26146 - Reassembling encrypted fragments with non-consecutive packet numbers
- CVE-2020-26147 - Reassembling mixed encrypted/plaintext fragments