Bern, 18.05.2021

Statement WLAN Fragattack

Der Sicherheitsforscher Mathy Vanhoef hat einige Probleme in der 802.11 WLAN-Implementation gefunden. Diese Themen werden unter dem Begriff Fragattack behandelt.

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

Die Attacken im Allgemeinen erlauben dem Angreifer:

- die Injektion von L2 Frames (abhängig vom Angriffsvektor) in ein verschlüsseltes WLAN-Netzwerk,
- das Ausfiltern von einigen Netzwerkdaten unter bestimmten Voraussetzungen.

Diese Angriffe zielen auf Schwachstelle im Fragmentation-Feature ab. Davon betroffen ist der Betrieb im Client und Access-Point Modus.

WLAN ohne Verschlüsselung (z.B. Public WiFi) sind von den Fragattack Schwachstellen nicht betroffen, da die kompromittierten Sicherheitsfunktion aufgrund der fehlenden Verschlüsselung nicht zur Anwendung kommen.

Die WLAN-Treiber aller NetModule Router sind von Fragattack betroffen. Deswegen stellt die Firma NetModule zeitnah für alle noch unterstützten Router folgende Releases bereit, um die Sicherheitslücken zu schliessen:

- 4.5.0.104
- 4.4.0.110
- 4.3.0.112

Für alle NetModule Geräte mit WLAN Features wird ein Software Update empfohlen.

Folgende CVEs werden mit den Updates adressiert:

- 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