IPmotion CAR-A-WAN Test für " FragAttacks " Sicherheitslücken am *27. Mai 2021*

1. Einführung

Dieses Dokument enthält unsere Testergebnisse für die "FragAttacks"-Schwachstellen, die in dem Papier *"Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation"* von Mathy Vanhoef veröffentlicht wurden. [1]

Die Tests wurden von unserem Mitarbeiter Malte Niemann mit den von Mathy Vanhoef zur Verfügung gestellten Werkzeugen durchgeführt. [2]

Die Dokumentation und weitere Informationen finden Sie auf der "FragAttack"-Website. [3]

2. Schwachstellen

Die folgenden Schwachstellen werden getestet:

CVE-2020-24588 : Aggregationsangriff (Akzeptieren von Nicht-SPP-A-MSDU-Frames).

CVE-2020-24587 : Angriff mit gemischten Schlüsseln (Wiederzusammensetzen von Fragmenten, die unter verschiedenen Schlüsseln verschlüsselt wurden).

CVE-2020-24586 : Fragment-Cache-Angriff (keine Löschung von Fragmenten aus dem Speicher bei (erneuter) Verbindung mit einem Netzwerk).

CVE-2020-26145 : Akzeptieren von Klartext-Broadcast-Fragmenten als vollständige Frames (in einem verschlüsselten Netzwerk).

CVE-2020-26144 : Akzeptieren von Klartext-A-MSDU-Frames, die mit einem RFC1042-Header mit EtherType EAPOL beginnen (in einem verschlüsselten Netzwerk).

CVE-2020-26140 : Akzeptieren von Klartext-Datenframes in einem geschützten Netzwerk.

CVE-2020-26143 : Akzeptieren von fragmentierten Klartext-Datenrahmen in einem geschützten Netzwerk.

CVE-2020-26139 : Weiterleitung von EAPOL-Frames, obwohl der Absender noch nicht authentifiziert ist (sollte nur APs betreffen).

---

[1] https://papers.mathyvanhoef.com/usenix2021.pdf

[2] https://github.com/vanhoefm/fragattacks

[3] https://www.fragattacks.com

CVE-2020-26146 : Wiederzusammensetzen von verschlüsselten Fragmenten mit nicht-fortlaufenden Paketnummern.

CVE-2020-26147 : Wiederzusammensetzen von gemischten Verschlüsselungs-/Klartextfragmenten.

CVE-2020-26142 : Verarbeitung von fragmentierten Frames als volle Frames.

CVE-2020-26141 : Keine Verifizierung der TKIP MIC von fragmentierten Frames.

3. Testaufbau

Der Testaufbau besteht aus einem Arch-Linux-System, das für die Unterstützung der aktualisierten WLAN-Treiber und der Test-Suite modifiziert wurde. Als Netzwerkkarte kommt die im Testhandbuch empfohlene und getestete TP-Link "TL-WN722N" zum Einsatz.

Der Test wird in der vorgeschlagenen Reihenfolge mit Hilfe des Python-Skripts fragattack.py ausgeführt.

4. Testpersonen

Die Testobjekte sind unsere mobilen WLAN-Router CAR-A-WAN v4 und CAR-A-WAN v6.

Der CAR-A-WAN v4 besteht aus einem v4-7e Board mit einem DNMA92 miniPCI wifi Modul.

Der CAR-A-WAN v6 besteht aus einem v6-5c4-Board mit einem Compex WLE600VX WiFi-Modul, das auf einem Qualcomm QCA9882 Chipsatz läuft.

Beide Testobjekte werden mit mehreren unserer internen Build-Versionen getestet, um Nebeneffekte mit anderen Komponenten zu verringern.

5. Testergebnisse

CAR-A-WAN v4

Schwachstelle	Testergebnis	Bedeutung
CVE-2020-24588	System unterstützt Nicht-SPP-AMSDUs. Injektionsangriffe sind zeitlich begrenzt.	Das System unterstützt nicht-SPP A-MSDUs, was es anfällig für Angriffe machen könnte. Der Referenzangriff funktioniert jedoch NICHT. Der fragmentierte Header wird verworfen und die Anfrage wird abgebrochen.
CVE-2020-24587	N/A	Angriffe mit gemischten Schlüsseln können auf unserem System nicht getestet werden, da es die Sitzungsschlüssel nicht zur Laufzeit erneuert.

CVE-2020-24586	Injektion erfolgreich.	Das System löscht den Speicher nicht aus den Fragmenten, wenn der Client sich erneut mit dem Netzwerk verbindet.
CVE-2020-26146	Injektion fehlgeschlagen.	Pakete können nicht mit nicht aufeinanderfolgenden Paketnummern gesendet werden.
CVE-202026147/26140/26143	Eine Injektion war erfolgreich. Der Rest schlug fehl.	Die meisten Mixed-Frame-Angriffe führen zu einem Timeout. Ein für Linux-Systeme spezifizierter Mixed-Frame-Angriff wird jedoch akzeptiert. Dies könnte eine große Schwachstelle sein, wie in 6.3 des Papiers angegeben, wenn sie in Kombination mit einem A-MSDU-Angriff oder einem Cache-Angriff verwendet wird.
CVE-2020-26145	Injektion fehlgeschlagen.	Broadcast-Klartext-Angriffe sind nicht erfolgreich.
CVE-2020-26144	Injektion fehlgeschlagen.	Getarnte A-MSDU, die als EAPOL-Frames getarnt sind, sind nicht erfolgreich.

CAR-A-WAN v6

Schwachstelle	Testergebnis	Bedeutung
CVE-2020-24588	System unterstützt Nicht-SPP-AMSDUs. Injektionen erfolgreich.	Das System unterstützt nicht-SPP A-MSDUs, was es anfällig für Angriffe machen könnte. A-MSDU-Injektionen sind erfolgreich, aber nur mit legalen Daten. Bad Parsing-Angriffe sind nicht erfolgreich.
CVE-2020-24587	N/A	Angriffe mit gemischten Schlüsseln können auf unserem System nicht getestet werden, da es die Sitzungsschlüssel nicht zur Laufzeit erneuert.
CVE-2020-24586	Injektion erfolgreich.	Das System löscht den Speicher nicht aus den Fragmenten, wenn der Client sich erneut mit dem Netzwerk verbindet.
CVE-2020-26146	Injektion erfolgreich.	Pakete können mit nicht fortlaufenden Paketnummern gesendet werden.
CVE-202026147/26140/26143	Injektion erfolgreich, wenn Startframe verschlüsselt ist.	Mixed-Frame-Angriffe funktionieren nur, wenn der Frame verschlüsselt beginnt. Frames, die im Klartext beginnen, werden abgewiesen.
CVE-2020-26145	Injektion fehlgeschlagen.	Broadcast-Klartext-Angriffe sind nicht erfolgreich.
CVE-2020-26144	Injektion fehlgeschlagen.	Getarnte A-MSDU, die als EAPOL-Frames getarnt sind, sind nicht erfolgreich.

6. Fazit

Unser CAR-A-WAN v4 ist anfällig für Cached-Fragment- sowie Mixed-Fragment-Angriffe, was es anfällig für eine breitere Palette von Angriffen macht. Es gibt weder für diese Version des Linux-Kernels noch für die Firmware des DNMA92-WLAN-Moduls einen Fix. Da es sich hierbei um unser älteres Produkt handelt, das sein EoL erreicht hat, gibt es keinen Fix, der implementiert werden könnte.

Das CAR-A-WAN v6 ist für die meisten Angriffe anfällig. Wir müssen unseren Kernel mit den Patches patchen, die über die Linux-Kernel-Community verfügbar sind. Es ist derzeit nicht bekannt, ob wir die Firmware-Treiber für die Wifi-Karten aktualisieren müssen. Es gibt derzeit keinen Patch (Stand 27. Mai 2021) für die ATH10k-Firmware-Version, die den Qualcomm-Chipsatz QCA9882 unterstützt. Wir müssen mit unseren Lieferanten kommunizieren, wenn sich dies ändern sollte.