Test IPmotion CAR-A-WAN pour les vulnérabilités " FragAttacks " le *27 mai 2021*

1. Introduction

Ce document fournit les résultats de nos tests pour les vulnérabilités "FragAttacks" qui ont été publiées dans le document *"Fragment and Forge : Breaking Wi-Fi Through Frame Aggregation and Fragmentation"* par Mathy Vanhoef. [1]

Les tests sont réalisés par notre employé Malte Niemann avec les outils fournis par Mathy Vanhoef. [2]

Pour la documentation et de plus amples informations, veuillez consulter le site web "FragAttack". [3]

2. Vulnérabilités

Les vulnérabilités suivantes sont testées :

CVE-2020-24588 : attaque par agrégation (acceptation de trames A-MSDU non-SPP).

CVE-2020-24587 : attaque par clé mixte (réassemblage de fragments chiffrés sous différentes clés).

CVE-2020-24586 : attaque du cache des fragments (ne pas effacer les fragments de la mémoire lors de la (re)connexion à un réseau).

CVE-2020-26145 : Acceptation de fragments de diffusion en clair comme trames complètes (dans un réseau crypté).

CVE-2020-26144 : Acceptation des trames A-MSDU en clair qui commencent par un en-tête RFC1042 avec EtherType EAPOL (dans un réseau crypté).

CVE-2020-26140 : Acceptation de trames de données en clair dans un réseau protégé.

CVE-2020-26143 : Acceptation de trames de données en texte clair fragmentées dans un réseau protégé.

CVE-2020-26139 : Transfert des trames EAPOL même si l'expéditeur n'est pas encore authentifié (ne devrait affecter que les AP).

CVE-2020-26146 : Réassemblage de fragments chiffrés avec des numéros de paquets non consécutifs.

CVE-2020-26147 : Réassemblage de fragments mixtes cryptés/plaintext.

---

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

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

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

CVE-2020-26142 : Traitement des trames fragmentées comme des trames complètes.

CVE-2020-26141 : Ne pas vérifier le MIC TKIP des trames fragmentées.

3. Configuration du test

La configuration de test consiste en un système Arch Linux qui a été modifié pour supporter les pilotes WLAN mis à jour et la suite de tests. La carte réseau utilisée est la TP-Link "TL-WN722N" qui est recommandée et testée par le manuel de test.

Le test est exécuté dans l'ordre suggéré en utilisant le script python fragattack.py.

4. Sujets d'essai

Les sujets de test sont nos routeurs WLAN mobiles CAR-A-WAN v4 et CAR-A-WAN v6.

Le CAR-A-WAN v4 se compose d'une carte v4-7e avec un module wifi miniPCI DNMA92.

Le CAR-A-WANv6 se compose d'une carte v6-5c4 avec un module wifi Compex WLE600VX fonctionnant avec un chipset Qualcomm QCA9882.

Les deux sujets de test sont testés avec plusieurs de nos versions de construction internes afin de diminuer les effets secondaires avec d'autres composants.

5. Résultats des tests

CAR-A-WAN v4

Vulnérabilité	Résultat du test	Signification
CVE-2020-24588	Le système prend en charge les AMSDU non-SPP. Les attaques par injection s'arrêtent.	Le système prend en charge les A-MSDU non-SPP, ce qui pourrait le rendre vulnérable aux attaques. Cependant, l'attaque par référence ne fonctionne PAS. L'en-tête fragmentée est abandonnée et la requête s'arrête.
CVE-2020-24587	N/A	Les attaques par clé mixte ne peuvent pas être testées sur notre système puisqu'il ne renouvelle pas les clés de session au moment de l'exécution.
CVE-2020-24586	Injection réussie.	Le système n'efface pas la mémoire des fragments lorsque le client se reconnecte au réseau.

CVE-2020-26146	L'injection a échoué.	Les paquets ne peuvent pas être envoyés avec des numéros de paquets non consécutifs.
CVE-202026147/26140/26143	Une injection a réussi. Les autres ont échoué.	La plupart des attaques par trames mixtes se terminent au bout du compte. Cependant, une attaque par trame mixte spécifiée pour les systèmes Linux est acceptée. Cela pourrait être une vulnérabilité majeure comme indiqué en 6.3 du document si elle est utilisée en combinaison avec une attaque A-MSDU ou une attaque de cache.
CVE-2020-26145	L'injection a échoué.	Les attaques par diffusion de texte en clair ne réussissent pas.
CVE-2020-26144	L'injection a échoué.	Les trames A-MSDU masquées comme des trames EAPOL n'aboutissent pas.

CAR-A-WAN v6

Vulnérabilité	Résultat du test	Signification
CVE-2020-24588	Le système prend en charge les AMSDU non-SPP. Injections réussies.	Le système prend en charge les A-MSDU non-SPP, ce qui pourrait le rendre vulnérable aux attaques. Les injections A-MSDU sont réussies mais seulement avec des données légales. Les attaques de mauvaise analyse syntaxique ne réussissent pas.
CVE-2020-24587	N/A	Les attaques par clé mixte ne peuvent pas être testées sur notre système puisqu'il ne renouvelle pas les clés de session en cours d'exécution.
CVE-2020-24586	Injection réussie.	Le système n'efface pas la mémoire des fragments lorsque le client se reconnecte au réseau.
CVE-2020-26146	Injection réussie.	Les paquets peuvent être envoyés avec des numéros de paquets non consécutifs.
CVE-202026147/26140/26143	Injection réussie si la trame de départ est cryptée.	Les attaques par trames mixtes ne fonctionnent que lorsque la trame commence par être chiffrée. Les trames commençant en clair sont refusées.
CVE-2020-26145	L'injection a échoué.	Les attaques par diffusion de texte en clair ne réussissent pas.
CVE-2020-26144	L'injection a échoué.	Les trames A-MSDU masquées comme des trames EAPOL n'aboutissent pas.

6. Conclusion

Notre CAR-A-WAN v4 est vulnérable aux attaques par fragment en cache ainsi qu'aux attaques par fragment mixte, ce qui le rend vulnérable à un plus large éventail d'attaques. Il n'y a pas de correctif pour cette version du noyau Linux ou pour le firmware du module wifi DNMA92. Puisqu'il s'agit de notre ancien produit et qu'il a atteint sa fin de vie, aucun correctif ne peut être implémenté.

Le CAR-A-WAN v6 est vulnérable à la plupart des attaques. Nous devrons mettre à jour notre noyau avec les correctifs disponibles via la communauté Linux kernel. Nous ne savons pas actuellement si nous devons mettre à jour les pilotes de firmware pour les cartes wifi. Il n'y a actuellement aucun patch (état le 27 mai 2021) pour la version du firmware ATH10k qui supporte le chipset Qualcomm QCA9882. Nous devrons communiquer avec nos fournisseurs si cela est susceptible de changer.