IPmotion CAR-A-WAN test for “FragAttacks” vulnerabilities on *May 27th 2021*

1. Introduction

This document provides our test results for the “FragAttacks” vulnerabilities that have been published in the paper *"Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation”* by Mathy Vanhoef.[1]

The tests are conducted by our employee Malte Niemann with the tools provided by Mathy Vanhoef.[2]

For documentation and more information please consult the “FragAttack” website.[3]

2. Vulnerabilities

The following vulnerabilities are tested:

CVE-2020-24588: aggregation attack (accepting non-SPP A-MSDU frames).

CVE-2020-24587: mixed key attack (reassembling fragments encrypted under different keys).

CVE-2020-24586: fragment cache attack (not clearing fragments from memory when (re)connecting to a network).

CVE-2020-26145: Accepting plaintext broadcast fragments as full frames (in an encrypted network).

CVE-2020-26144: Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network).

CVE-2020-26140: Accepting plaintext data frames in a protected network.

CVE-2020-26143: Accepting fragmented plaintext data frames in a protected network.

CVE-2020-26139: Forwarding EAPOL frames even though the sender is not yet authenticated (should only affect APs).

CVE-2020-26146: Reassembling encrypted fragments with non-consecutive packet numbers.

CVE-2020-26147: Reassembling mixed encrypted/plaintext fragments.

CVE-2020-26142: Processing fragmented frames as full frames.

CVE-2020-26141: Not verifying the TKIP MIC of fragmented frames.

---

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

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

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

3. Test setup

The test setup consists of an Arch Linux system that has been modified to support the updated WLAN drivers and test suite. The network card in use is the TP-Link "TL-WN722N" that is recommended and tested by the testing manual.

The test is run in the suggested order by using the fragattack.py python script.

4. Test subjects

The test subjects are our mobile WLAN routers CAR-A-WAN v4 and CAR-A-WAN v6.

The CAR-A-WAN v4 consists of a v4-7e Board with a DNMA92 miniPCI wifi module.

The CAR-A-WAN v6 consists of a v6-5c4 Board with a Compex WLE600VX wifi module that runs on a Qualcomm QCA9882 chipset.

Both test subjects are tested with multiple of our internal build versions to diminish side effects with other components.

5. Test results

CAR-A-WAN v 4

Vulnerability	Test result	Meaning
CVE-2020-24588	System supports non-SPP A-MSDUs. Injection attacks time out.	The system supports non-SPP A-MSDUs which could make it vulnerable to attacks. However, the reference attack is NOT working. The fragmented header gets dropped and the request times out.
CVE-2020-24587	N/A	Mixed key attacks cannot be tested on our system since it does not renew session keys at runtime.
CVE-2020-24586	Injection successful.	The system is not clearing memory from fragments when client reconnects to the network.
CVE-2020-26146	Injection failed.	Packets cannot be sent with non-consecutive packet numbers.
CVE-2020-26147/26140/26143	One injection succeeded. The rest failed.	Most mix frame attacks time out. However a mixed frame attack specified for Linux systems is accepted. This could be a major vulnerability like stated in 6.3 of the paper if used in combination with either a A-MSDU attack or a cache attack.
CVE-2020-26145	Injection failed.	Broadcast plaintext attacks are not successful.
CVE-2020-26144	Injection failed.	Cloaked A-MSDU cloaked as EAPOL frames are not successful.

CAR-A-WAN v6

Vulnerability	Test result	Meaning
CVE-2020-24588	System supports non-SPP A-MSDUs. Injections successful.	The system supports non-SPP A-MSDUs which could make it vulnerable to attacks. A-MSDU injections are successful but only with legal data. Bad parsing attacks are not successful.
CVE-2020-24587	N/A	Mixed key attacks cannot be tested on our system since it does not renew session keys in runtime.
CVE-2020-24586	Injection successful.	The system is not clearing memory from fragments when client reconnects to the network.
CVE-2020-26146	Injection successful.	Packets can be sent with non-consecutive packet numbers.
CVE-2020-26147/26140/26143	Injection successful if starting frame is encrypted.	Mixed frame attacks only work when the frame is starting encrypted. Frames starting in plaintext are refused.
CVE-2020-26145	Injection failed.	Broadcast plaintext attacks are not successful.
CVE-2020-26144	Injection failed.	Cloaked A-MSDU cloaked as EAPOL frames are not successful.

6. Conclusion

Our CAR-A-WAN v4 is vulnerable to cached fragment as well as mixed fragment attacks which makes it vulnerable to a wider array of attacks. There is no fix for either this version of the Linux kernel or the DNMA92 wifi module firmware. Since this is our legacy product and has reached it's EOL there is no fix that could be implemented.

The CAR-A-WAN v6 is vulnerable to most of the attacks. We will need to patch our kernel with the patches that are available via the Linux kernel community. It's currently not known if we need to update the firmware drivers for the wifi cards. There is currently no patch (state May 27th 2021) for the ATH10k firmware version that supports the Qualcomm QCA9882 chipset. We will need to communicate with our suppliers if this is subject to change.