Application Report

FragAttacks - FRagmentation and AGgregation Attacks

TI-PSIRT-2020-090066

Publication date: May 11, 2021

Summary

TI PSIRT has analyzed a series of aggregation and fragmentation attacks against Wi-Fi® devices as published by Mathy Vanhoef and found that TI Wi-Fi components in the CC3xxx and WL18xx families are potentially vulnerable only to a subset of the attacks as listed in the table below. These attacks could potentially lead to issues such as injection of arbitrary packets.

CVEID	Description	CVSS score	CVSS vector	WL18xx NLCP	WL18xx MCP	CC31xx/ CC32xx
CVE-2020-24588	Accepting non-SPP A-MSDU frames: The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2 and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SPP A-MSDU frames, which is mandatory as part of 802.11n, an adversary can abuse this to inject arbitrary network packets.	5.9	#CVSS:3.1/AV:A/ AC:H/PR:N/ UI:N/S:U/C:N/I:H/A:L	Vulnerable	Vulnerable	Vulnerable
CVE-2020-26146	Reassembling encrypted fragments with non-consecutive packet numbers: Vulnerable WPA, WPA2 or WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP or GCMP data-confidentiality protocol is used. Note that WEP is considered vulnerable and should not be used.	3.1	#CVSS:3.1/AV:A/ AC:H/PR:N/ UI:N/S:U/C:N/I:L/A:N	Vulnerable	Vulnerable	Not vulnerable
CVE-2020-26140	Accepting plaintext data frames in a protected network: Vulnerable WEP, WPA, WPA2 or WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	7.1	#CVSS:3.1/ AV:A/AC:L/PR:N/ UI:N/S:U/C:N/I:H/A:L	Not vulnerable	Vulnerable in Access Point role only	Vulnerable in Access Point role only
CVE-2020-26143	Accepting fragmented plaintext data frames in a protected network: Vulnerable WEP, WPA, WPA2 or WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.	7.1	#CVSS:3.1/ AV:A/AC:L/PR:N/ UI:N/S:U/C:N/I:H/A:L	Not vulnerable	Vulnerable in Access Point role only	Vulnerable in Access Point role only

These attacks require physical proximity to the target Wi-Fi devices.

Affected products and versions

- SimpleLink™ Wi-Fi CC323x / CC313x Service Pack 4.9.0.2_3.7.0.1_3.1.0.26 and older
- SimpleLink™ Wi-Fi CC322x / CC312x Service Pack 3.18.0.2_2.7.0.0_2.2.0.7 and older
- SimpleLink™ Wi-Fi CC320x / CC310x Service Pack 1.0.1.15-2.13.0.2 and older
- WL18xx FW version 8.9.0.0.87 and older

Suggested mitigations

TI has released software updates for both product families that address these potential vulnerabilities. It is recommended that customers apply the software updates as they become available. The updates have been released in the following deliverable versions:

- SimpleLink Wi-Fi CC323x / CC313x Service Pack 4.10.0.1_3.7.0.1_3.1.0.26
  - Could be downloaded from the following link: https://www.ti.com/tool/SIMPLELINK-CC32XX-SDK
- SimpleLink Wi-Fi CC322x / CC312x Service Pack 3.19.0.1_2.7.0.0_2.2.0.7
  - Could be downloaded from the following link: https://www.ti.com/tool/SIMPLELINK-CC32XX-SDK
- SimpleLink Wi-Fi CC320x / CC310x Service Pack 1.0.1.15-2.14.0.0
  - Could be downloaded from the following links: https://www.ti.com/tool/download/CC3200SDK / https://www.ti.com/tool/download/CC3100SDK
- WL18xx FW version 8.9.0.0.88
  - Could be downloaded from the following link: https://git.ti.com/cgit/wilink8-wlan/wl18xx_fw/tree/

Below are more technical details about the released fixes:

CVE-2020-24588 (Aggregation)

Exhibits the following behaviors:

Discard all subframes in an A-MSDU if its 1st subframe exhibits any one of the following behaviors:

- DA does not match its own 802.11 header RA in FromDS frame
- SA does not match 802.11 header TA in ToDS frame
- DA is AA:AA:03:00:00:00 or DA is AA:AA:03:00:00:F8 (Any DS bits including 4-addr)
- Incorrect SNAP header in the subframe

CVE-2020-26146 (Reassembling encrypted fragments with non-consecutive packet numbers)

Exhibits the following behaviors:

- During defragmentation, the PN shall have strict increment of 1 for consecutive fragments

CVE-2020-26140 (Accepting plaintext data frames in a protected network)

Exhibits the following behaviors:

- Plaintext data frames shall be discarded when encryption is expected in a protected network

CVE-2020-26143 (Accepting fragmented plaintext data frames in a protected network)

Exhibits the following behaviors:

- When a MSDU or MMPDU is encrypted, every fragment from the respective MSDU/MMPDU is expected to be encrypted and any unencrypted fragments shall be discarded

Revision History

Changes from Revision * (May 2021) to Revision A (May 2021)	Page
• Added "CVSS score" and "CVSS vector" columns to table	1
• Removed "and are complicated to exploit" from attack description	1

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (https:www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265