Information note

Topic **Frame Aggregation vulnerability (Frag attacks) on Wi-Fi modules**

UBX-21028740 C1-Public

Author Hari Vigneswaran

Date 2 July 2021

1 Affected products

Product series	Product name	Ordering code	Type no.	Remarks
EMMY-W1	All	All	All	
ELLA-W1	All	All	All	
JODY-W1	All	All	All	
JODY-W2	All	All	All	
LILY-W1	All	All	All	
NINA-W10	All	All	All	
NINA-W13	All	All	All	
NINA-W15	All	All	All	
ODIN-W2	All	All	All	

2 Issue description

Wi-Fi alliance recently disclosed a new set of vulnerabilities relating to fragmentation and reassembly of frames over Wi-Fi. Hackers can exploit this vulnerability to inject malicious packets into a Wi-Fi network and in some rare cases, exfiltrate data from the network. All devices that implement Wi-Fi frame fragmentation and re-assembly are vulnerable.

The CVE entries for these vulnerabilities are:

- CVE-2020-24586
- CVE-2020-24587
- CVE-2020-24588
- CVE-2020-26139
- CVE-2020-26140
- CVE-2020-26141
- CVE-2020-26142
- CVE-2020-26143
- CVE-2020-26144
- CVE-2020-26145

- CVE-2020-26146
- CVE-2020-26147

According to the Wi-Fi alliance, there is no documented evidence of the vulnerabilities having been exploited in real-world scenarios.

3 Recommendations against FRAG vulnerability

The u-blox Wi-Fi team has concluded that all the above-mentioned products are vulnerable to some type of FRAG attacks. All customers are recommended to update their device firmware to protect against FRAG attacks.

For JODY-W1 a patch is already available from Infineon. Customers can download the latest firmware version for PCIe or SDIO that resolves this vulnerability from the Infineon web site or contact u-blox directly:

- PCIe Wi-Fi Firmware Version 9.40.117.28 based on the 'Clutch' release
- SDIO Wi-Fi Firmware Version 9.40.112.21 based on the 'Brakepad' release

For JODY-W2, EMMY-W1, LILY-W1, and ELLA-W1 u-blox is awaiting a patch from NXP.

For NINA-W10, patches have already been released by Espressif. Customers are requested to update their application to include the patches from here.

For NINA-W13, NINA-W15 and ODIN-W2, u-blox is currently working on a release that fixes the problem.

4 General Security Recommendations

Customers are always advised to enable security protocols on a higher layer e.g., Transport Layer Security (TLS) to protect all data packets end-to-end.

Customers are always advised to use only the latest Wi-Fi security protocols like WPA3.

u-blox periodically releases software that includes security patches. Customers are advised to periodically update the firmware of the device to protect their products from security vulnerabilities.

Customers are requested to contact their local u-blox sales representative with any related questions or support enquiries.

5 Reference documents

[1] Security Advisory from Wi-Fi alliance
[2] FRAG attack technical information