Information note

Topic **u-blox Bluetooth modules affected by SweynTooth vulnerability**

UBX-20028561 C1-Public

Author Hari Vigneswaran

Date 12 April 2021

1 Affected products

Product series	Product name	Ordering code	Type no.	Remarks
JODY-W1	All	All	All	
R41Z	All	All	All	
JODY-W2	All	All	All	
EMMY-W1	All	All	All	

2 Type of change

☐ Hardware modification
☒ Firmware update
☐ Documentation update
☐ Others

3 Description of change

A group of Singaporean researchers have reported a group of Bluetooth vulnerabilities denoted as SweynTooth. The CVE entries for these vulnerabilities are:

- CVE-2019-16336
- CVE-2019-17519
- CVE-2019-17517
- CVE-2019-17518
- CVE-2019-17520
- CVE-2019-19195
- CVE-2019-19196
- CVE-2019-17061
- CVE-2019-17060
- CVE-2019-19192
- CVE-2019-19193
- CVE-2019-19194

Sweyntooth captures a family of 12 vulnerabilities across different Bluetooth Low Energy (LE) software development kits (SDKs) of seven major system-on-a-chip (SoC) vendors. The vulnerabilities expose flaws in specific Bluetooth LE SoC implementations that allows an attacker in radio range to trigger deadlocks, crashes, and buffer overflows or completely bypass security depending on the circumstances.

The u-blox Bluetooth team has completed an investigation on all variants of the following product series: NINA-B1, NINA-B2, NINA-B3, NINA-B4, NINA-W1, BMD-30, BMD-33, BMD-35, BMD-34, BMD-36, BMD-38, ANNA-B1, ODIN-W2, R41Z, OBS-421, ELLA-W1, EMMY-W1, JODY-W1 and JODY-W2.

- JODY-W1 has been identified vulnerable to CVE-2019-16336, CVE-2019-17519, CVE-2019-17060, CVE-2019-17061, CVE-2019-17517, CVE-2019-19193 and CVE-2019-19195. A new firmware (patch-RAM update) is available for JODY-W1 series. Customers can obtain the latest version CYW89359B1_002.002.014.0153 from u-blox.
- R41Z has been identified vulnerable to CVE-2019-17061, CVE-2019-17060, CVE-2019-16336 and CVE-2019-17519. A patched Bluetooth stack (2.2.1) has been released by NXP Semiconductors for R41Z.
- EMMY-W1 has been identified vulnerable to CVE-2019-19193. New firmware versions for SD-UART (W15.87.19.p44-15.100.19.p44-C4X15675_A2-MGPL) and SD-SD (W15.68.19.p48-15.26.19.p48-C4X15687_A2-MGPL) with the fix are available from u-blox.
- JODY-W2 has been identified vulnerable to CVE-2019-19193. New firmware versions for SD-UART (W16.87.10.p137-16.16.10.p137-C4X16687-MGPL) and SD-SD (W16.68.10.p139-16.16.10.p139-C4X16687-MGPL) with the fix are available from u-blox.
- EMMY-W1 has been identified vulnerable to CVE-2019-19193. New firmware versions for SD-UART (W15.87.19.p44-15.100.19.p44-C4X15675_A2-MGPL) and SD-SD (W15.68.19.p48-15.26.19.p48-C4X15687_A2-MGPL) with the fix is available from u-blox.
- NINA-B1, NINA-B2, NINA-B3, NINA-B4, NINA-W1, BMD-30, BMD-33, BMD-35, BMD-34, BMD-36, BMD-38, ANNA-B1, ODIN-W2, OBS-421 and ELLA-W1 are not affected by the vulnerability.

4 Schedule

A patch is already available for all the affected products.

5 Customer impact and recommended action

- Customers should update the firmware of the module to resolve the identified vulnerability as soon as possible.
- In case of questions, customers are requested to contact their corresponding sales representative for support.

6 Reference documents

[1] SweynTooth vulnerabilities list
[2] NXP mcuxpresso SDK
[3] ICS Alert (ICS-ALERT-20-063-01)