Information note

Topic **Bluetooth security vulnerability - BLURtooth**

UBX-20039433 C1-Public

Author Erik Carlberg

Date 18 September 2020

1 Affected products

Product name	Ordering code	Type number	Software	Remarks
ANNA-B112	All	All	All	
BMD-3xx	All	All	N/A	
NINA-B11x	All	All	All	
NINA-B22x	All	All	All	
NINA-B3xx	All	All	All	
NINA-W10x	All	All	All	
NINA-W15x	All	All	All	
OBS421	All	All	All	
ODIN-W26x	All	All	All	
R41Z	All	All	N/A	
JODY-W16x	All	All	All	
JODY-W26x	All	All	All	
JODY-W37x	All	All	All	
EMMY-W1xx	All	All	All	

2 Type

- ☐ Product status change
- ☐ Hardware/component change
- ☐ Firmware/software update
- ☐ Label change
- ☐ Documentation update
- ☐ Certification information
- ☒ Security advisory
- ☐ Other

3 Description

Researchers at the École Polytechnique Fédérale de Lausanne (EPFL) and Purdue University have independently identified vulnerabilities related to Cross-Transport Key Derivation (CTKD) in implementations supporting pairing and encryption with both Bluetooth BR/EDR and LE in Bluetooth Specifications 4.2 through 5.0. The research identified that CTKD, when implemented to older versions of the specification, may permit escalation of access between the two transports with non-authenticated encryption keys replacing authenticated keys or weaker encryption keys replacing stronger encryption keys.

This vulnerability is dubbed BLURtooth and reported as CVE-2020-15802. It is further described by the Bluetooth SIG and CERT Coordination Center.

4 Impact on u-blox products

4.1 ANNA-B1, BMD-3, NINA-B1, NINA-B3 and R41Z

BLURtooth vulnerability requires both Bluetooth Low Energy as well as Bluetooth BR/EDR (aka Bluetooth Classic). Since the modules in this section support only Bluetooth Low Energy, they are not affected by BLURtooth.

4.2 NINA-B2, NINA-W1, OBS421 and ODIN-W2

The Cross-Transport Key Derivation (CTKD) functionality is not supported by the modules in this section and hence they are not affected by the BLURtooth vulnerability.

4.3 JODY-W1, JODY-W2, JODY-W3 and EMMY-W1

The Cross-Transport Key Derivation (CTKD) functionality is enabled by the host Bluetooth stack. Customers are requested to check with the host stack vendor and make sure to patch the BLURtooth vulnerability. There are no changes to the controller software/firmware.

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

5 Reference documents

[1] Bluetooth SIG Statement on BLURtooth

[2] Vulnerability Note: Carnegie Mellon University