Product change note

Topic **NINA-B2/W13/W15 bootloader update**
UBX-19051875

Author Erik Carlberg

Date 3 December 2019

1 Affected products

Product name	Order code	Type number (old)	Type number (new)	Software
NINA-B221	NINA-B221-00B	NINA-B221-00B-00	NINA-B221-00B-01	u-connectXpress 1.0
NINA-B222	NINA-B222-00B	NINA-B222-00B-00	NINA-B222-00B-01	u-connectXpress 1.0
NINA-W131	NINA-W131-00B	NINA-W131-00B-01	NINA-W131-00B-02	u-connectXpress 1.0
NINA-W132	NINA-W132-00B	NINA-W132-00B-01	NINA-W132-00B-02	u-connectXpress 1.0
NINA-W131	NINA-W131-01B	NINA-W131-01B-00	NINA-W131-01B-01	u-connectXpress 2.0
NINA-W132	NINA-W132-01B	NINA-W132-01B-00	NINA-W132-01B-01	u-connectXpress 2.0
NINA-W151	NINA-W151-00B	NINA-W151-00B-00	NINA-W151-00B-01	u-connectXpress 1.0
NINA-W152	NINA-W152-00B	NINA-W152-00B-00	NINA-W152-00B-01	u-connectXpress 1.0

2 Type of change

☐ Hardware modification
☒ Software update
☐ Documentation update
☐ Others

3 Description of change

u-blox has identified weaknesses in the Espressif ESP32 chip used in the listed modules relating to the vulnerability reports CVE-2019-15894 and CVE-2019-17391. These issues affect the security of bootloader integrated in modules. An attacker with physical access to the modules may be able to extract cryptographic information from the Espressif chip and inject non-intended software that could further compromise the module functionality.

To mitigate the effect of the reported vulnerabilities, the bootloader in the listed products is redesigned resulting in a more secure key generation procedure.

A complete remedy of the identified vulnerabilities is pending availability of an updated ROM code in the ESP32 chip. Espressif has announced that this is in progress and u-blox intends to release another update of the affected products as soon as the new ROM code version of the ESP32 chip is available.

4 Schedule

Shipment of parts with the new type number is estimated to start from January 10, 2020. This date is pending inventory depletion and may be affected by fluctuations in supply and demand.

Consequently, although customers should be prepared to receive the changed product on this date, u-blox will continue to ship pre-changed products until a time in which inventory has been depleted. This may result in pre-changed product being shipped to customers after this forecasted date.

5 Customer impact and recommended action

The bootloader protocol is unchanged and the update is fully transparent for the user of the module.

Once this change is effective, customers placing orders on the existing ordering codes, will receive the modules with updated bootloader automatically.

In general, customers are advised to review security requirements for their end-devices with this vulnerability in mind. Actions could include ensuring that the Wi-Fi/Bluetooth module is not accessible for unauthorized physical access, tampering and reverse engineering or prevent unauthorized software updates to the vulnerable modules in the field.

The vulnerability cannot be addressed via a software upgrade, upgraded modules have to be installed in order to address the vulnerability.

6 Reference documents

[1] NINA-B2 data sheet, doc. no. UBX-18006649
[2] NINA-W13 data sheet, doc. no. UBX-17006694
[3] NINA-W15 data sheet, doc. no. UBX-18006647
[4] NINA-B2 system integration manual, doc. no. UBX-18011096
[5] NINA-W1 system integration manual, doc. no. UBX-17005730
[6] u-connect AT commands manual, doc. no. UBX-14044127
[7] u-blox bootloader protocol specification, doc. no. UBX-17065404