Information note

Topic **Fault injection vulnerability in Bluetooth LE modules with nRF52 chips**
UBX-20029495

Author Hari Vigneswaran

Date 29 June 2020

1 Affected products

Product name	Ordering code	Type no.	Remarks
ANNA-B112	All	All	SiP design can offer some increased resilience, see Product considerations
BMD-300 BMD-301	All	All	
BMD-330	All	All	
BMD-340 BMD-341 BMD-345	All	All	
BMD-350	All	All	
BMD-360	All	All	
BMD-380	All	All	
NINA-B111 NINA-B112	All	All	Pre-flashed bootloader can offer some increased resilience, see Product considerations
NINA-B301 NINA-B302 NINA-B306	All	All	
NINA-B400 NINA-B406	All	All	Pre-flashed bootloader can offer some increased resilience, see Product considerations

2 Issue description

Nordic Semiconductor has recently identified [1] a potentially malicious fault injection technique that makes nRF52-series of Bluetooth Low Energy (LE) chips vulnerable to a particular type of side-channel attack.

Hackers can exploit this vulnerability to circumvent the APPROTECT functionality and enable the debug interface during that active power cycle. However, physical access to the chip and some tampering with specific hardware components is required to successfully exploit this vulnerability.

Nordic nRF52 series of chips are used in a range of u-blox Bluetooth LE modules. Some u-blox modules are more vulnerable than others to this type of attack.

3 Mitigations and recommended actions

3.1 Design considerations

- Prevent, as much as possible, physical access to the Bluetooth module.
- In new designs, do not route the SWD pins out anywhere on the PCB.
- Store secrets and private keys in an external Secure Element (SE) and not onboard the nRF52 chips.
- Follow other applicable security best practices. For example, rotate keys periodically, do not use the same secret key on more than one device, etc.

3.2 Product considerations

NINA-B1, ANNA-B1 and NINA-B40 series can offer some increased resilience to this kind of attack:

- The ANNA-B1 SiP design makes any physical access to the module components more difficult. This is likely to prolong any attempted fault injection attack.
- NINA-B1, ANNA-B1 and NINA-B40 modules are provided with a pre-flashed bootloader. This allows customers to flash any software over a serial UART interface – rather than over the SWD interface. Customers can thus avoid routing out the SWD pins anywhere on their PCB.

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

4 Reference documents

[1] Nordic Semiconductors, Information Notice (IN-133 v1.0)