Informational Notice (IN)

IN no.:	**IN-133 v1.0**	Date:	**2020-06-12**
Device affected:	**nRF52 series**	Device version / Build Code:	**All versions**

Description:

A fault injection technique that causes failure of logical access port protection mechanisms on nRF52-series devices has been identified and was disclosed by an independent party on June 10th, 2020.

The technique drives the device into invalid states of operation, which are non-destructive, but cause functional failure of device configuration parameters at boot. By repeating this technique and analysis over a large range of permutations, the functional failure can be targeted at the APPROTECT configuration resulting in debug port connectivity and function. At this point, the debugger has access to the device memory and registers.

Consequence:

Failure of the APPROTECT configuration and debug port connectivity and function implies access to all memory on a device. A device that programmatically configured APPROTECT can have that configuration circumvented and program memory containing program instructions can be read out of the device. It is also possible to write to memory.

Identifying affected implementations:

This technique is known to be effective on all nRF52 series devices.

Mitigations:

Preventing physical access to the device, or detecting and responding to product enclosure breach, are mitigations for fault injection techniques.

Further information:

Fault injection refers to physical tampering with operational conditions outside of specified range in order to drive device logic levels into invalid states and then investigate how the device malfunctions. Voltage glitching, extreme temperatures, and electro-magnetic pulse (EMP) injection can be used to create conditions for such logic failure.

Once a fault injection has been found to cause a malfunction, an attacker can investigate if that malfunction is somehow able to be exploited. This is a process of trial-and-error and can require hundreds or thousands of attempts. If a fault sequence is found that causes a malfunction that can be exploited, then the attack is re-producible.

Fault injection techniques can employ relatively low-cost equipment. The design of an attack would likely incorporate this equipment and software to control fault signals with precision and test for malfunction behaviors. It requires complete physical access to a device, a detailed understanding of microcontrollers and in-depth knowledge of the device being attacked.

Other physical attacks which result in extraction of code or circuit information can also be applied, but often require specialized equipment at a higher cost.

The nRF52-series of SoCs, like many standard microcontroller circuits, are not hardened against fault injection techniques.

First disclosure date:

2020-06-10

Attachments: ☒ No ☐ Yes – describe:

Technical contact at Nordic Semiconductor:

Contact: Technical Support Team at
www.nordicsemi.com, "Support"

Commercial contact at Nordic Semiconductor:

Contact: Account Regional Sales Manager:
www.nordicsemi.com, "Contact Us"

Authorization for Nordic Semiconductor

Product Manager	Date:	2020-06-12	Sign:	Kjetil Holstad
Quality Director	Date:	2020-06-12	Sign:	

Nordic Semiconductor ASA
P.O. Box 2336
7004 Trondheim
Norway
Tel.: +47 72 89 89 00