Nordic Semiconductor ASA
Otto Nielsens vei 12, N-7004 Trondheim, Norway
Phone: +47 72 89 89 00 Fax: +47 72 89 89 89
Reg. nr./VAT no.: 966011726

Informational Notice of Security Vulnerability (IN)

Notice no.: IN-119, rev. 1.0.1

Date: 2019-08-12

Affected products:
BLE SoftDevices released prior to July 2016

Product version information:
All versions of S110, S120 and S130
S132 v2.0.0

Description:

A security vulnerability affecting nRF51 Bluetooth Low Energy software stacks was disclosed by an independent person at the DEF CON hacker conference on August 11, 2019. The vulnerability requires a non-compliant BLE protocol stack to send invalid, or mal-formed packets in response to request types generated by a GATT Client implementation. This vulnerability is not exposed by qualified implementations of BLE protocol stacks that implement valid behavior.

The disclosure provided details on how the attacker was able to corrupt and manipulate device memory, and referenced source codes used by the reporter. The disclosure limited information on exploiting the vulnerability to a specific implementation of a wireless USB dongle and custom application Software.

Consequence:
If an attacker implements a Bluetooth protocol stack that can construct invalid or mal-formed packets toward an nRF51 BLE stack, the attacker may provoke an error where a packet buffer, located in RAM allocated on the call stack, is overrun and corrupted.

Identifying affected implementations:
This issue exists in BLE protocol stacks released before July 2016.

Affected implementations must have the following criteria:

- Use an affected BLE protocol stack
- Use a GATT Client
- Execute a service discovery procedure or a read of a characteristic by UUID which results in one of the following request packet types to be sent to a device implementing a GATT server:
  - READ_BY_TYPE_REQUEST
  - READ_BY_GROUP_TYPE_REQUEST

Implementations using Central Role are likely to execute a service discovery procedure. If an implementation uses Peripheral Role only, GATT Client is optionally implemented.

Consequence / Impact / Severity:

The following behaviors can be provoked by an attacker depending on the content of invalid packets and the level of prior knowledge an attacker has about the memory map of an application.

- The device may continuously write to RAM addresses until a CPU fault occurs. This may be observed as an unresponsive application and/or a reset of an application.
- Partial corruption of call stack memory and continued execution may occur. The observed behavior is not predictable and dependent on the application. Data corruption of received packets is likely.
- Partial corruption of memory and manipulation of instruction execution is a potential result of a sophisticated attack where prior knowledge or experimental knowledge of memory contents, protocol packet exchanges, and application functions could be used to target instruction insertion and provoke specific behavior.

The impact on an application can be high, rendering it non-functional until a reset occurs to reload software. The severity ranges from low, recoverable on reset, to high, if instructions can be injected for execution.

In the case of instruction insertion, the attack requires prior knowledge of a specific application and may or may not succeed based on several protocol exchange sequence and timing factors which may be outside the control of the attacker.

Solution:

All users are recommended to use the latest release of BLE protocol stack software for product development. All BLE protocol stacks from Nordic Semiconductor released after July 2016 are not affected by this vulnerability.

Nordic Semiconductor ASA
Otto Nielsens vei 12, N-7004 Trondheim, Norway
Phone: +47 72 89 89 00 Fax: +47 72 89 89 89
Reg. nr./VAT no.: 966011726

Informational Notice Security Vulnerability (IN)

Further information:

This vulnerability was not identified in 2016, but resolved as a result of re-implementation of packet buffer handling at that time.

Products based on nRF52 series devices and BLE protocol stacks with release date after July 2016 do not contain the vulnerability and cannot be exploited by this attack.

Qualified Bluetooth implementations do not provoke the exploitation of this vulnerability and do not cause any behavior associated with this vulnerability.

If you are a customer of Nordic Semiconductor which may have a product affected by this security vulnerability, and you would like to discuss the issue with us, please contact your Regional Sales Manager.

First disclosure date:	**Solution availability date:**
2019-08-11	July 2016

Attachments: ☒ No ☐ Yes

Technical contact at Nordic Semiconductor:	**Commercial contact at Nordic Semiconductor:**
Contact: Technical support team www.nordicsemi.com , “Support”	Contact: Account Regional Sales Manager www.nordicsemi.no , “Contact Us”

Authorization for Nordic Semiconductor

Product Manager	Date:	2019-08-12	Sign:	
Quality Director	Date:	2019-08-12	Sign: