Product Security Advisory

HID

nRF52 Fault Injection

TLP:WHITE

No Restriction on Distribution

HID-PSA-2020-02

11-November-2020

Overview:

Nordic Semiconductor has identified a fault injection attack that may allow an unauthorized individual to bypass the APPROTECT feature of the nRF52 chipset family and reactivate the debug interface on all nRF52 chipsets. An attack of this nature may enable an attacker to write to the device's memory, allow the attacker to read the memory of the nRF52 device, or allow the installation of a malicious variation of the device's firmware on the device. For more information, please refer to the Nordic Semiconductor Information Notice[1].

HID initiated an investigation immediately following Nordic's announcement, and this investigation is ongoing. Based on HID's investigation to date and on Nordic Semiconductor's disclosures, this type of attack requires physical access to the nRF52 chip mounted on the PCB within the reader enclosure.

Affected Products:

The following HID products use nRF52 series chips:

1. HID® iCLASS SE® Express R10
2. HID® iCLASS SE® RB25F
3. HID® Signo™ Readers (models 20, 40, 20K, 40K)

Mitigation:

Nordic Semiconductor's disclosure states that "[p]reventing physical access to the device, or detecting and responding to product enclosure breach, are mitigations for fault injection techniques."

Because execution of a potential attack requires physical access to the nRF52 chip, HID recommends mitigating this risk by taking the following actions consistent with Nordic Semiconductor's guidance:

1. Enable, monitor, and investigate reader tamper alarms designed to alert when a reader has been removed from the mounting surface and
2. Use the security screw to connect the reader to the mounting plate and

3. Update the reader firmware or reinstall the latest version to reset any unauthorized firmware changes.

Next Steps:

HID continues to investigate the vulnerability and will provide an update should it determine that additional mitigation measures are reasonably necessary.

Contact Information:

If you have additional questions or suspect that a reader has been compromised, please contact HID Technical Support at https://www.hidglobal.com/support

References:

[1] Nordic Semiconductor’s announcement for information can be obtained directly from the manufacturer at https://infocenter.nordicsemi.com/pdf/in_133_v1.0.pdf.