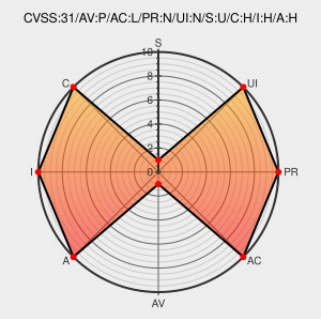
CVE-2020-27208

Published on: 05/21/2021 12:00:00 AM UTC

Last Modified on: 05/28/2021 03:41:00 PM UTC

CVE-2020-27208

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fido2 from Nitrokey contain the following vulnerability:

The flash read-out protection (RDP) level is not enforced during the device initialization phase of the SoloKeys Solo 4.0.0 & Somu and the Nitrokey FIDO2 token. This allows an adversary to downgrade the RDP level and access secrets such as private ECC keys from SRAM via the debug interface.

CVE-2020-27208 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Solo – SoloKeys	solokeys.com text/html	MISC solokeys.com
Security and Trust in Open	www.aisec.fraunhofer.de	MISC www.aisec.fraunhofer.de/de/das-institut/wissenschaftliche-

Security and Trust in Open Source Security Tokens - Fraunhofer AISEC	text/html	MISC www.aisec.fraunhofer.de/de/das-institut/wissenschaftliche-exzellenz/security-and-trust-in-open-source-security-tokens.html
SoloKeys (@SoloKeysSec) | Twitter	nitter.domain.glass text/html	MISC twitter.com/SoloKeysSec
patches to improve resistance to fault injection · solokeys/solo@a9c02cd · GitHub	github.com text/html	MISC github.com/solokeys/solo/commit/a9c02cd354f34b48195a342c7f524abdef5cbcec
Cryptology ePrint Archive: Report 2021/640 - Security and Trust in Open Source Security Tokens	eprint.iacr.org text/html	MISC eprint.iacr.org/2021/640
Shedding too much Light on a Microcontroller's Firmware Protection - Fraunhofer AISEC	www.aisec.fraunhofer.de text/html	MISC www.aisec.fraunhofer.de/en/FirmwareProtection.html

Related QID Numbers

750836 OpenSUSE Security Update for solo (openSUSE-SU-2021:1019-1)

Exploit/POC from Github

PoC for exploiting CVE-2020-27208

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nitrokey	Fido2	-	All	All	All
Operating System	Nitrokey	Fido2 Firmware	-	All	All	All
Hardware	Solokeys	Solo	-	All	All	All
Operating System	Solokeys	Solo Firmware	4.0.0	All	All	All
Hardware	Solokeys	Somu	-	All	All	All
Operating System	Solokeys	Somu Firmware	-	All	All	All

cpe:2.3:h:nitrokey:fido2:-:*:*:*:*:*:*:*:

cpe:2.3:o:nitrokey:fido2_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:solokeys:solo:-:*:*:*:*:*:*:*:

cpe:2.3:o:solokeys:solo_firmware:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:h:solokeys:somu:-:*:*:*:*:*:*:*:

cpe:2.3:o:solokeys:somu_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-27208 : The flash read-out protection RDP level is not enforced during the device initialization phase o… twitter.com/i/web/status/1…	2021-05-21 12:06:25
/r/netcve	CVE-2020-27208	2021-05-21 12:41:38

← Previous ID

Next ID→