



CVE-2021-29415

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-29415
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-21 12:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	The elliptic curve cryptography (ECC) hardware accelerator, part of the ARM® TrustZone® CryptoCell 310, contained in the

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nordicsemi	Nrf52840	-	All	All	All
Operating System	Nordicsemi	Nrf52840 Firmware	All	All	All	All

References

Reference	Source	Link
CVE - Fraunhofer SIT	MISC	www.sit.fraunhofer.de
Security and Trust in Open Source Security Tokens - Fraunhofer AISEC	MISC	www.aisec.fraunhofer.de
Cryptology ePrint Archive: Report 2021/640 - Security and Trust in Open Source Security Tokens	MISC	eprint.iacr.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)