CVE-2023-40271

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-40271
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-08 02:15:00 UTC
Updated	2023-09-13 02:27:00 UTC
Description	In Trusted Firmware-M through TF-Mv1.8.0, for platforms that integrate the CryptoCell accelerator, when the CryptoCell PS

Risk And Classification

Problem Types: CWE-697

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Trusted Firmware-m	1.6.0	All	All	All
Application	Arm	Trusted Firmware-m	1.6.1	All	All	All
Application	Arm	Trusted Firmware-m	1.7.0	All	All	All
Application	Arm	Trusted Firmware-m	1.8.0	All	All	All

References

Reference
cc3xx_partial_tag_compare_on_chacha20_poly1305.rst « security_advisories « security « docs - trusted-firmware-m.git - Trusted Firmware fo
Releases — Trusted Firmware-M v1.6.1 documentation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report