CVE-2020-25082

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25082
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-10 17:15:00 UTC
Updated	2021-08-17 17:48:00 UTC
Description	An attacker with physical access to Nuvoton Trusted Platform Module (NPCT75x 7.2.x before 7.2.2.0) could extract an Ellip

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nuvoton	Npct75x	-	All	All	All
Operating System	Nuvoton	Npct75x Firmware	All	All	All	All

References

Reference	Sourc
SA-002: Potential Extraction of an Elliptic Curve Cryptography (ECC) private key via a side-channel attack against ECDSA - Nuvoton	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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