Nuvoton - CWE-1300: Improper Protection of Physical Side Channels

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

Summary

CVE	CVE-2026-6923
State	PUBLISHED
Assigner	INCD
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 17:16:24 UTC
Updated	2026-05-14 17:16:24 UTC
Description	A side-channel attack, which requires a physical presence to the TPM, can lead to extraction of an Elliptic Curve Diffie-Hellr

Risk And Classification

Primary CVSS: v3.1 3.8 LOW from cna@cyber.gov.il

CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-1300 | CWE-1300 CWE-1300 Improper protection of physical side channels

Version	Source	Type	Score	Severity	Vector
3.1	cna@cyber.gov.il	Secondary	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Physical

Attack Complexity
High

Privileges Required
High

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity

Integrity

None

Availability

None

CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nuvoton	NPCT7xx	affected all versions below 7.2.4.0 cpe	Not specified

References

Reference	Source	Link	Tags
www.gov.il/en/departments/dynamiccollectors/cve_advisories_listing	cna@cyber.gov.il	www.gov.il	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Robin Muller, Roman Korkikian - uSec (en)

Additional Advisory Data

Solutions

CNA: Upgrade to version 7.2.4.0 or above.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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.

Free CVE JSON API cve.report/api

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