CVE-2026-41990

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

Summary

CVE	CVE-2026-41990
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 05:16:05 UTC
Updated	2026-04-23 05:16:05 UTC
Description	Libgcrypt before 1.12.2 mishandles Dilithium signing. Writes to a static array lack a bounds check but do not use attacker-c

Risk And Classification

Primary CVSS: v3.1 4 MEDIUM from cve@mitre.org

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

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gnupg	Libgcrypt	affected 1.12.0 1.12.2 semver	Not specified

References

Reference	Source	Link	Tags
lists.gnupg.org/pipermail/gnupg-announce/2026q2/000503.html	cve@mitre.org	lists.gnupg.org	
www.openwall.com/lists/oss-security/2026/04/21/1	cve@mitre.org	www.openwall.com	
dev.gnupg.org/T8208	cve@mitre.org	dev.gnupg.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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