Out-of-Bounds Read in mgcore_SH_25_3!aligned_free()

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

Summary

CVE	CVE-2026-32864
State	PUBLISHED
Assigner	NI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 20:16:26 UTC
Updated	2026-04-13 14:52:36 UTC
Description	There is a memory corruption vulnerability due to an out-of-bounds read in mgcore_SH_25_3!aligned_free() in NI LabVIEW

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from security@ni.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000160000 probability, percentile 0.036220000 (date 2026-04-15)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds read

Version	Source	Type	Score	Severity	Vector
4.0	security@ni.com	Secondary	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	security@ni.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ni	Labview	2023	q1	All	All
Application	Ni	Labview	2023	q3	All	All
Application	Ni	Labview	2023	q3_patch1	All	All

Application	Ni	Labview	2023	q3_patch2	All	All
Application	Ni	Labview	2023	q3_patch3	All	All
Application	Ni	Labview	2023	q3_patch4	All	All
Application	Ni	Labview	2023	q3_patch5	All	All
Application	Ni	Labview	2023	q3_patch6	All	All
Application	Ni	Labview	2023	q3_patch7	All	All
Application	Ni	Labview	2023	q3_patch8	All	All
Application	Ni	Labview	2024	-	All	All
Application	Ni	Labview	2024	q1	All	All
Application	Ni	Labview	2024	q1_patch1	All	All
Application	Ni	Labview	2024	q3	All	All
Application	Ni	Labview	2024	q3_patch1	All	All
Application	Ni	Labview	2024	q3_patch2	All	All
Application	Ni	Labview	2024	q3_patch3	All	All
Application	Ni	Labview	2024	q3_patch4	All	All
Application	Ni	Labview	2024	q3_patch5	All	All
Application	Ni	Labview	2025	q1	All	All
Application	Ni	Labview	2025	q1_patch1	All	All
Application	Ni	Labview	2025	q1_patch2	All	All
Application	Ni	Labview	2025	q1_patch3	All	All
Application	Ni	Labview	2025	q3	All	All
Application	Ni	Labview	2025	q3_patch1	All	All
Application	Ni	Labview	2025	q3_patch2	All	All
Application	Ni	Labview	2025	q3_patch3	All	All
Application	Ni	Labview	2026	q1	All	All
Application	Ni	Labview	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NI	LabVIEW	affected 23.0.0 semver	Not specified
CNA	NI	LabVIEW	affected 23.1.0 23.3.9 semver	Not specified
CNA	NI	LabVIEW	affected 24.1.0 24.3.6 semver	Not specified
CNA	NI	LabVIEW	affected 25.1.0 25.3.4 semver	Not specified
CNA	NI	LabVIEW	affected 26.1.0 26.1.1 semver	Not specified

References

Reference	Source	Link	Tags
www.ni.com/en/support/security/available-critical-and-security-updates-f...	security@ni.com	www.ni.com	Vendor Advisory
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: Michael Heinzl (en)

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