CVE-2026-40385

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

Summary

CVE	CVE-2026-40385
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-12 19:16:20 UTC
Updated	2026-04-14 20:15:39 UTC
Description	In libexif through 0.6.25, an unsigned 32bit integer overflow in Nikon MakerNote handling could be used by local attackers t

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

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

EPSS: 0.000120000 probability, percentile 0.018220000 (date 2026-04-15)

Problem Types: CWE-190 | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
3.1	cve@mitre.org	Secondary	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L
3.1	CNA	CVSS	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libexif Project	Libexif	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Libexif Project	Libexif	affected 0.6.25 semver	Not specified

References

Reference	Source	Link	Tags
github.com/libexif/libexif/commit/93003b93e50b3d259bd2227d8775b73a53c35d58	cve@mitre.org	github.com	Patch
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.