CVE-2026-40386

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

Summary

CVE	CVE-2026-40386
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 20:43:44 UTC
Description	In libexif through 0.6.25, an integer underflow in size checking for Fuji and Olympus MakerNote decoding could be used by

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-191 | CWE-191 CWE-191 Integer Underflow (Wrap 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/dc6eac6e9655d14d0779d99e82d0f5f442d2f34b	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.

© 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**