



# CVE-2026-40385

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-40385
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-12 19:16:20 UTC
<b>Updated</b>	2026-04-14 20:15:39 UTC
<b>Description</b>	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

Integrity

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	<a href="#">Libexif Project</a>	<a href="#">Libexif</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Libexif Project</a>	<a href="#">Libexif</a>	affected 0.6.25 semver	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://github.com/libexif/libexif/commit/93003b93e50b3d259bd2227d8775b73a53c35d58">github.com/libexif/libexif/commit/93003b93e50b3d259bd2227d8775b73a53c35d58</a>	<a href="mailto:cve@mitre.org">cve@mitre.org</a>	<a href="https://github.com">github.com</a>	Patch
CVE Program record	<a href="https://www.cve.org">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="https://nvd.nist.gov">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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 registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)