



OpenEXR has a misaligned write in LossyDctDecoder_execute leading to undefined behavior (DWA/DWAB decompression)

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-34379 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-06 16:16:35 UTC |
| Updated | 2026-04-07 19:04:50 UTC |
| Description | OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the r |

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from security-advisories@github.com

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

EPSS: 0.000330000 probability, percentile 0.095690000 (date 2026-04-07)

Problem Types: CWE-704 | CWE-787 | CWE-843 | CWE-704 CWE-704: Incorrect Type Conversion or Cast | CWE-787 CWE-787: Out-of-bounds Write | CWE-843 CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1 | security-advisories@github.com | Secondary | 7.1 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H |
| 3.1 | CNA | DECLARED | 7.1 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Openexr | Openexr | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------------------------|---------|----------------------------|---------------|
| CNA | AcademySoftwareFoundation | Openexr | affected >= 3.2.0, < 3.2.7 | Not specified |
| CNA | AcademySoftwareFoundation | Openexr | affected >= 3.3.0, < 3.3.9 | Not specified |
| CNA | AcademySoftwareFoundation | Openexr | affected >= 3.4.0, < 3.4.9 | Not specified |

References

| Reference | Source | Link | Tags |
|---|--------------------------------|--------------|-----------|
| github.com/AcademySoftwareFoundation/openexr/releases/tag/v3.2.7 | security-advisories@github.com | github.com | Product |
| github.com/AcademySoftwareFoundation/openexr/releases/tag/v3.3.9 | security-advisories@github.com | github.com | Product |
| github.com/AcademySoftwareFoundation/openexr/releases/tag/v3.4.9 | security-advisories@github.com | github.com | Product |
| github.com/AcademySoftwareFoundation/openexr/security/advisories/GHSA-w8... | security-advisories@github.com | github.com | Exploit |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical |

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 registered 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