OpenEXR has a signed 32-bit Overflow in PIZ Decoder Leads to OOB Read/Write

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

Summary

CVE	CVE-2026-34588
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 19:01:21 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: v4.0 8.6 HIGH from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/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: 0.000140000 probability, percentile 0.024600000 (date 2026-04-07)

Problem Types: CWE-125 | CWE-190 | CWE-787 | CWE-125 CWE-125: Out-of-bounds Read | CWE-190 CWE-190: Integer Overflow or Wraparound | CWE-787 CWE-787: Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/S
4.0	CNA	DECLARED	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/S
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/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

None

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:N/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 >= 3.1.0, <= 3.1.13	Not specified
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	Produc
github.com/AcademySoftwareFoundation/openexr/releases/tag/v3.3.9	security-advisories@github.com	github.com	Produc
github.com/AcademySoftwareFoundation/openexr/releases/tag/v3.4.9	security-advisories@github.com	github.com	Produc
github.com/AcademySoftwareFoundation/openexr/security/advisories/GHSA-58...	security-advisories@github.com	github.com	Exploit,
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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