



# OpenImageIO: Integer overflow in QueryRGBBufferSizeInternal leads to heap out-of-bounds write in DPX decoder (kCbYCr and kABGR)

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

## Summary

<b>CVE</b>	CVE-2026-43907
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-14 20:17:06 UTC
<b>Updated</b>	2026-05-15 19:43:22 UTC
<b>Description</b>	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / anima

## Risk And Classification

**Primary CVSS:** v3.1 8.3 HIGH from security-advisories@github.com

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

**EPSS:** 0.000390000 probability, percentile 0.119130000 (date 2026-05-16)

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

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H
3.1	CNA	DECLARED	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

High

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openimageio	Openimageio	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AcademySoftwareFoundation	OpenImageIO	affected < 3.0.18.0	Not specified
CNA	AcademySoftwareFoundation	OpenImageIO	affected >= 3.1.4.0-beta, < 3.1.13.0	Not specified

#### References

Reference	Source	Link
github.com/AcademySoftwareFoundation/OpenImageIO/security/advisories/GHS...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)