



CVE-2020-15306

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

Summary

CVE	CVE-2020-15306
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-26 01:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in ge

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Openexr	Openexr	All	All	All	All
Application	Openexr	Openexr	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference

Debian -- Security Information -- DSA-4755-1 openexr

openexr/CHANGES.md at master · AcademySoftwareFoundation/openexr · GitHub

[SECURITY] Fedora 32 Update: mingw-OpenEXR-2.4.1-2.fc32 - package-announce - Fedora Mailing-Lists

OpenEXR: Multiple vulnerabilities (GLSA 202107-27) — Gentoo security

[security-announce] openSUSE-SU-2020:0970-1: moderate: Security update f

always ignore chunkCount attribute unless it cannot be computed by peterhillman · Pull Request #738 · AcademySoftwareFoundation/openexr

[SECURITY] Fedora 32 Update: mingw-OpenEXR-2.4.1-2.fc32 - package-announce - Fedora Mailing-Lists

openexr/SECURITY.md at master · AcademySoftwareFoundation/openexr · GitHub

[SECURITY] Fedora 31 Update: mingw-OpenEXR-2.3.0-4.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2358-1] openexr security update

[security-announce] openSUSE-SU-2020:1015-1: moderate: Security update f

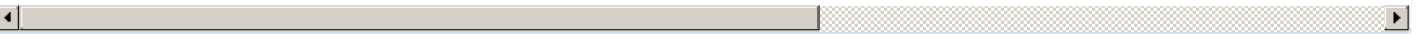
[SECURITY] Fedora 31 Update: mingw-OpenEXR-2.3.0-4.fc31 - package-announce - Fedora Mailing-Lists

Release v2.5.2 · AcademySoftwareFoundation/openexr · GitHub

USN-4418-1: OpenEXR vulnerabilities | Ubuntu security notices | Ubuntu

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501101](#) Alpine Linux Security Update for openexr

[501647](#) Alpine Linux Security Update for openexr

[672178](#) EulerOS Security Update for openexr (EulerOS-SA-2022-2475)

[710048](#) Gentoo Linux OpenEXR Multiple Vulnerabilities (GLSA 202107-27)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)