



# CVE-2021-3479

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

## Summary

<b>CVE</b>	CVE-2021-3479
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-31 14:15:00 UTC
<b>Updated</b>	2022-12-13 01:56:00 UTC
<b>Description</b>	There's a flaw in OpenEXR's Scanline API functionality in versions before 3.0.0-beta. An attacker who is able to submit a cr

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Openexr</a>	<a href="#">Openexr</a>	All	All	All	All
Application	<a href="#">Openexr</a>	<a href="#">Openexr</a>	All	All	All	All

## References

Reference	Source	Link
25370 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	<a href="#">bugs.chro</a>
OpenEXR: Multiple vulnerabilities (GLSA 202107-27) — Gentoo security	GENTOO	<a href="#">security.g</a>
[SECURITY] [DLA 3236-1] openexr security update	MLIST	<a href="#">lists.debia</a>
[SECURITY] [DLA 2701-1] openexr security update	MLIST	<a href="#">lists.debia</a>
1939149 – (CVE-2021-3479) CVE-2021-3479 OpenEXR: Out-of-memory caused by allocation of a very large buffer	MISC	<a href="#">bugzilla.re</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

174984	SUSE Enterprise Linux Security Update for openexr (SUSE-SU-2021:1489-1)
178693	Debian Security Update for openexr (DLA 2701-1)
180300	Debian Security Update for openexr (CVE-2021-3479)
181315	Debian Security Update for openexr (DLA 3236-1)
198318	Ubuntu Security Notification for Openexr Vulnerabilities (USN-4900-1)
501648	Alpine Linux Security Update for openexr
502133	Alpine Linux Security Update for openexr
672178	EulerOS Security Update for openexr (EulerOS-SA-2022-2475)
690438	Free Berkeley Software Distribution (FreeBSD) Security Update for openexr, ilmbase (98044aba-6d72-11eb-aed7-1b1b8a70cc8b)
710048	Gentoo Linux OpenEXR Multiple Vulnerabilities (GLSA 202107-27)
750230	OpenSUSE Security Update for openexr (openSUSE-SU-2021:0670-1)
750712	SUSE Enterprise Linux Security Update for openexr (SUSE-SU-2021:2159-1)

© [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](#)