



CVE-2020-15389

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

Summary

CVE	CVE-2020-15389
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-29 21:15:00 UTC
Updated	2022-10-06 17:59:00 UTC
Description	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and in

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Oracle	Outside In Technology	8.5.4	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
Application	Oracle	Outside In Technology	8.5.4	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	Third
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
Heap use-after-free · Issue #1261 · uclouvain/openjpeg · GitHub	MISC	github.com	Patch
Debian -- Security Information -- DSA-4882-1 openjpeg2	DEBIAN	www.debian.org	
OpenJPEG: Multiple vulnerabilities (GLSA 202101-29) — Gentoo security	GENTOO	security.gentoo.org	Third
> [Suggested description]> jp2/opj_decompress.c in OpenJPEG through 2.3.1 has - Pastebin.com	MISC	pastebin.com	Third

[SECURITY] [DLA 2277-1] openjpeg2 security update	MLIST	lists.debian.org	Mailin
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159478 Oracle Enterprise Linux Security Update for openjpeg2 (ELSA-2021-4251)
178518 Debian Security Update for openjpeg2 (DSA 4882-1)
199240 Ubuntu Security Notification for OpenJPEG Vulnerabilities (USN-5952-1)
239842 Red Hat Update for openjpeg2 (RHSA-2021:4251)
296072 Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)
353122 Amazon Linux Security Advisory for openjpeg2 : ALAS2-2022-1741
500472 Alpine Linux Security Update for openjpeg
504229 Alpine Linux Security Update for openjpeg
670492 EulerOS Security Update for openjpeg2 (EulerOS-SA-2021-2250)
670518 EulerOS Security Update for openjpeg2 (EulerOS-SA-2021-2276)
670551 EulerOS Security Update for openjpeg2 (EulerOS-SA-2021-2309)
751971 SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:1129-1)
752044 SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:1252-1)
752060 SUSE Enterprise Linux Security Update for openjpeg (SUSE-SU-2022:1296-1)
940171 AlmaLinux Security Update for openjpeg2 (ALSA-2021:4251)
960346 Rocky Linux Security Update for openjpeg2 (RLSA-2021:4251)

© [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](#)