



CVE-2020-27843

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

Summary

CVE	CVE-2020-27843
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-05 18:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	A flaw was found in OpenJPEG in versions prior to 2.4.0. This flaw allows an attacker to provide specially crafted input to th

Risk And Classification

Problem Types: CWE-125

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	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All

References

Reference	Source
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
Oracle Critical Patch Update Advisory - July 2021	N/A
[SECURITY] [DLA 2975-1] openjpeg2 security update	MLIST
1907516 – (CVE-2020-27843) CVE-2020-27843 openjpeg: out-of-bounds read in opj_t2_encode_packet function in openjp2/t2.c	MISC
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists	
Debian -- Security Information -- DSA-4882-1 openjpeg2	DEBIAN

OpenJPEG: Multiple vulnerabilities (GLSA 202101-29) — Gentoo security	GENTOO
Oracle Critical Patch Update Advisory - April 2021	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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)
179181 Debian Security Update for openjpeg2 (DLA 2975-1)
199240 Ubuntu Security Notification for OpenJPEG Vulnerabilities (USN-5952-1)
239842 Red Hat Update for openjpeg2 (RHSA-2021:4251)
296069 Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)
353122 Amazon Linux Security Advisory for openjpeg2 : ALAS2-2022-1741
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)
752740 SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:3802-1)
752745 SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:3801-1)
752823 SUSE Enterprise Linux Security Update for openjpeg (SUSE-SU-2022:4082-1)
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](#)