



CVE-2020-27844

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

Summary

CVE	CVE-2020-27844
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's src/lib/openjp2/t2.c in versions prior to 2.4.0. This flaw allows an attacker to provide crafted

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	8.5.5	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All

References

Reference	Score
1907521 – (CVE-2020-27844) CVE-2020-27844 openjpeg: heap-based buffer overflow in opj_t2_encode_packet function in openjp2/t2.c	Medium
Oracle Critical Patch Update Advisory - July 2021	None
OpenJPEG: Multiple vulnerabilities (GLSA 202101-29) — Gentoo security	Good
[SECURITY] [DLA 2550-1] openjpeg2 security update	Medium
Oracle Critical Patch Update Advisory - April 2021	Medium
CVE Program record	Confidential
NVD vulnerability detail	None

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296069 Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)

500474 Alpine Linux Security Update for openjpeg

501814 Alpine Linux Security Update for chromium

501910 Alpine Linux Security Update for qt5-qtwebengine

504231 Alpine Linux Security Update for openjpeg

504609 Alpine Linux Security Update for chromium

505349 Alpine Linux Security Update for qt5-qtwebengine

690203 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (f00b65d8-7ccb-11eb-b3be-e09467587c17)

750325 OpenSUSE Security Update for chromium (openSUSE-SU-2021:0392-1)

© [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](#)