



# CVE-2020-27845

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

## Summary

<b>CVE</b>	CVE-2020-27845
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-05 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	There's a flaw in src/lib/openjp2/pi.c of openjpeg in versions prior to 2.4.0. If an attacker is able to provide untrusted input to

## Risk And Classification

### Problem Types: CWE-125

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Outside In Technology</a>	8.5.5	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	All	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	All	All	All	All

## References

Reference
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists
Oracle Critical Patch Update Advisory - July 2021
1907523 – (CVE-2020-27845) CVE-2020-27845 openjpeg: heap-based buffer overflow in functions opj_pi_next_rlcp, opj_pi_next_rplc and opj_pi_next_rplc
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists
Debian -- Security Information -- DSA-4882-1 openjpeg2
OpenJPEG: Multiple vulnerabilities (GLSA 202101-29) — Gentoo security

[SECURITY] [DLA 2550-1] openjpeg2 security update

Oracle Critical Patch Update Advisory - April 2021

CVE Program record

NVD vulnerability detail

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)

[198299](#) Ubuntu Security Notification for Openjpeg2 Vulnerabilities (USN-4880-1)

[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)

[671668](#) EulerOS Security Update for openjpeg (EulerOS-SA-2022-1751)

[671854](#) EulerOS Security Update for openjpeg (EulerOS-SA-2022-1907)

[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](#)