



CVE-2020-27814

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-27814 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-01-26 18:15:00 UTC |
| Updated | 2022-10-07 02:22:00 UTC |
| Description | A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files. An attacker could use this flaw to |

Risk And Classification

Problem Types: CWE-122

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 | Uclouvain | Openjpeg | All | All | All | All |
| Application | Uclouvain | Openjpeg | All | All | All | All |
| Application | Uclouvain | Openjpeg | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|-------------------------|
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www |
| 1901998 – (CVE-2020-27814) CVE-2020-27814 openjpeg: Heap-buffer-overflow in lib/openjp2/mqc.c could result in DoS | MISC | bugz |
| Debian -- Security Information -- DSA-4882-1 openjpeg2 | DEBIAN | www |
| OpenJPEG: Multiple vulnerabilities (GLSA 202101-29) — Gentoo security | GENTOO | secu |
| [SECURITY] [DLA 2550-1] openjpeg2 security update | MLIST | lists.c |
| Heap-buffer-overflow in lib/openjp2/mqc.c:499 · Issue #1283 · uclouvain/openjpeg · GitHub | MISC | github |
| CVE Program record | CVE.ORG | www |
| NVD vulnerability detail | NVD | nvd.r |

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 |
| 500473 Alpine Linux Security Update for openjpeg |
| 504230 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) |
| 752740 SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:3802-1) |
| 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](#)