CVE-2022-1122

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1122
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-29 18:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	A flaw was found in the opj2_decompress program in openjpeg2 2.4.0 in the way it handles an input directory with a large n

Risk And Classification

Problem Types: CWE-665

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	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Uclouvain	Openjpeg	2.4.0	All	All	All

References

Reference
2067052 – (CVE-2022-1122) CVE-2022-1122 openjpeg: segmentation fault in opj2_decompress due to uninitialized pointer
[SECURITY] Fedora 34 Update: openjpeg2-2.4.0-4.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: mingw-openjpeg2-2.4.0-5.fc35 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal - Access to 24x7 support and knowledge
Exist a issues of freeing uninitialized pointer in src/bin/jp2/opj_decompress.c , that will cause a segfault · Issue #1368 · uclouvain/openjpeg · G
[SECURITY] Fedora 36 Update: openjpeg2-2.4.0-10.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: mingw-openjpeg2-2.4.0-5.fc35 - package-announce - Fedora Mailing-Lists
OpenJPEG: Multiple Vulnerabilities (GLSA 202209-04) — Gentoo security
[SECURITY] Fedora 34 Update: openjpeg2-2.4.0-4.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2975-1] openjpeg2 security update

[SECURITY] Fedora 36 Update: openjpeg2-2.4.0-10.fc36 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal - Access to 24x7 support and knowledge

Red Hat Customer Portal - Access to 24x7 support and knowledge

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160253 Oracle Enterprise Linux Security Update for openjpeg2 (ELSA-2022-7645)

160292 Oracle Enterprise Linux Security Update for openjpeg2 (ELSA-2022-8207)

179181 Debian Security Update for openjpeg2 (DLA 2975-1)

184393 Debian Security Update for openjpeg2 (CVE-2022-1122)

20317 Oracle Database 21c Critical Patch Update - January 2023

20318 Oracle Database 19c Critical Patch Update - January 2023

20319 Oracle Database 19c Critical OJVM Patch Update - January 2023

240849 Red Hat Update for openjpeg2 (RHSA-2022:7645)

240863 Red Hat Update for openjpeg2 (RHSA-2022:8207)

282541 Fedora Security Update for mingw (FEDORA-2022-9515529c96)

282583 Fedora Security Update for mingw (FEDORA-2022-2d112d4480)

354122 Amazon Linux Security Advisory for openjpeg2 : ALAS2-2022-1894

354320 Amazon Linux Security Advisory for openjpeg2 : ALAS2022-2022-184

354458 Amazon Linux Security Advisory for openjpeg2 : ALAS2022-2022-122

355194 Amazon Linux Security Advisory for openjpeg2 : ALAS2023-2023-040

502228 Alpine Linux Security Update for openjpeg

504233 Alpine Linux Security Update for openjpeg

671901 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1941)

671923 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-2004)

671932 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1974)

671993 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-2140)

672008 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-2165)

710617 Gentoo Linux OpenJPEG Multiple Vulnerabilities (GLSA 202209-04)

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)

940739 AlmaLinux Security Update for openjpeg2 (ALSA-2022:7645)

940800 AlmaLinux Security Update for openjpeg2 (ALSA-2022:8207)

960458 Rocky Linux Security Update for openjpeg2 (RLSA-2022:7645)

960624 Rocky Linux Security Update for openjpeg2 (RLSA-2022:8207)

© 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 registred 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