CVE-2020-27842

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27842
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	There's a flaw in openjpeg's t2 encoder in versions prior to 2.4.0. An attacker who is able to provide crafted input to be proc

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
Application	Fedoraproject	Extra Packages For Enterprise Linux	7.0	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	Fedoraproject	Fedora Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Oracle	Outside In Technology	8.5.5	All	All	All
Application	Redhat	Codeready Linux Builder	8.0	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Codeready Linux Builder For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	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
[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
1907513 – (CVE-2020-27842) CVE-2020-27842 openjpeg: null pointer dereference in opj_tgt_reset function in lib/openjp2/tgt.c	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

671151 EulerOS Security Update for openjpeg2 (EulerOS-SA-2021-2808)

671455 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1433)

671470 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1454)

671526 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1492)

671539 EulerOS Security Update for openjpeg2 (EulerOS-SA-2022-1511)

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)