CVE-2020-27823

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27823
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-13 15:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	A flaw was found in OpenJPEG's encoder. This flaw allows an attacker to pass specially crafted x,y offset input to OpenJPE

Risk And Classification

Problem Types: CWE-787 | CWE-120

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	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: openjpeg2-2.3.1-9.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: openjpeg2-2.3.1-10.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
1905762 – (CVE-2020-27823) CVE-2020-27823 openjpeg: Heap-buffer-overflow write in lib-openjp2	MISC	bugzilla.redhat.com
Debian -- Security Information -- DSA-4882-1 openjpeg2	DEBIAN	www.debian.org
[SECURITY] Fedora 33 Update: openjpeg2-2.3.1-9.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2550-1] openjpeg2 security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)
- 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)
- 670583 EulerOS Security Update for openjpeg (EulerOS-SA-2021-2341)
- 670656 EulerOS Security Update for openjpeg (EulerOS-SA-2021-2414)
- 670720 EulerOS Security Update for openjpeg (EulerOS-SA-2021-2478)
- 671139 EulerOS Security Update for openjpeg (EulerOS-SA-2021-2601)
- 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)
- 752060 SUSE Enterprise Linux Security Update for openjpeg (SUSE-SU-2022:1296-1)
- 940171 AlmaLinux Security Update for openjpeg2 (ALSA-2021:4251)
- 960346 Rocky Linux Security Update for openjpeg2 (RLSA-2021:4251)