CVE-2021-4156

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4156
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-23 20:15:00 UTC
Updated	2023-09-29 13:15:00 UTC
Description	An out-of-bounds read flaw was found in libsndfile's FLAC codec functionality. An attacker who is able to submit a specially

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	Libsndfile Project	Libsndfile	1.1.10	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3126-1] libsndfile security update	MLIST	lists.debian.o
[SECURITY] [DLA 3058-1] libsndfile security update	MLIST	lists.debian.o
flac: Fix improper buffer reusing by yuawn · Pull Request #732 · libsndfile/libsndfile · GitHub	MISC	github.com
2027690 – (CVE-2021-4156) CVE-2021-4156 libsndfile: heap out-of-bounds read in src/flac.c in flac_buffer_copy	MISC	bugzilla.redh
Heap-buffer-overflow in src/flac.c:274:41 in flac_buffer_copy · Issue #731 · libsndfile/libsndfile · GitHub	MISC	github.com
libsndfile: Multiple Vulnerabilities (GLSA 202309-11) — Gentoo security	GENTOO	security.gent
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

159833 Oracle Enterprise Linux Security Update for libsndfile (ELSA-2022-1968)

179770 Debian Security Update for libsndfile (DLA 3058-1)

181101 Debian Security Update for libsndfile (DLA 3126-1)

182226 Debian Security Update for libsndfile (CVE-2021-4156)

240300 Red Hat Update for libsndfile (RHSA-2022:1968)

354267 Amazon Linux Security Advisory for libsndfile : ALAS2022-2022-175

354328 Amazon Linux Security Advisory for libsndfile : ALAS2022-2022-026

354819 Amazon Linux Security Advisory for libsndfile : ALAS2-2023-1998

355213 Amazon Linux Security Advisory for libsndfile : ALAS2023-2023-028

671826 EulerOS Security Update for libsndfile (EulerOS-SA-2022-1899)

671891 EulerOS Security Update for libsndfile (EulerOS-SA-2022-1936)

671957 EulerOS Security Update for libsndfile (EulerOS-SA-2022-2000)

671958 EulerOS Security Update for libsndfile (EulerOS-SA-2022-1970)

671997 EulerOS Security Update for libsndfile (EulerOS-SA-2022-2160)

671998 EulerOS Security Update for libsndfile (EulerOS-SA-2022-2135)

672211 EulerOS Security Update for libsndfile (EulerOS-SA-2022-2620)

710754 Gentoo Linux libsndfile Multiple Vulnerabilities (GLSA 202309-11)

751578 SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2022:0034-1)

751587 SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2022:0052-1)

751592 OpenSUSE Security Update for libsndfile (openSUSE-SU-2022:0052-1)

751750 OpenSUSE Security Update for libsndfile (openSUSE-SU-2022:0052-2)

753360 SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2022:14872-1)

940549 AlmaLinux Security Update for libsndfile (ALSA-2022:1968)

960316 Rocky Linux Security Update for libsndfile (RLSA-2022:1968)

CVE.report and Source URL Uptime Status status.cve.report