CVE-2020-36430

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-36430
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-20 07:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	libass 0.15.x before 0.15.1 has a heap-based buffer overflow in decode_chars (called from decode_font and process_text)

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Libass Project	Libass	All	All	All	All

References

Reference	Source	Link	Tag
oss-fuzz-vulns/OSV-2020-2099.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.com	
26674 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	
[SECURITY] Fedora 34 Update: libass-0.15.2-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
decode_font: fix subtraction broken by change to unsigned type · libass/libass@0171374 · GitHub	MISC	github.com	
[SECURITY] Fedora 34 Update: libass-0.15.2-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
libass: Denial of service (GLSA 202208-13) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

282522 Fedora Security Update for libass (FEDORA-2022-2af150223a)

710586 Gentoo Linux libass Denial of Service (DoS) Vulnerability (GLSA 202208-13)

750984 SUSE Enterprise Linux Security Update for libass (SUSE-SU-2021:2792-1)

751007 OpenSUSE Security Update for libass (openSUSE-SU-2021:1174-1)

751020 OpenSUSE Security Update for libass (openSUSE-SU-2021:2792-1)

Free CVE JSON API cve.report/api

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