CVE-2016-6832

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

Summary

CVE	CVE-2016-6832
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-15 19:59:00 UTC
Updated	2023-11-07 02:34:00 UTC
Description	Heap-based buffer overflow in the ff_audio_resample function in resample.c in libav before 11.4 allows remote attackers to

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libav	Libav	All	All	All	All

References

Reference	Source	Link	Tags
git.libav.org Git - libav.git/commit		git.libav.org	
libav: heap-based buffer overflow in ff_audio_resample (resample.c) | agostino's blog	MISC	blogs.gentoo.org	Exploit, Third Par
oss-security - Re: libav: heap-based buffer overflow in ff_audio_resample (resample.c)	MLIST	www.openwall.com	Exploit, Mailing Li
Bug 825 – Invalid memory writes with libavresample	CONFIRM	bugzilla.libav.org	Exploit, Issue Tra
oss-security - libav: heap-based buffer overflow in ff_audio_resample (resample.c)	MLIST	www.openwall.com	Exploit, Mailing Li
git.libav.org Git - libav.git/commit	CONFIRM	git.libav.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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