CVE-2019-12730

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

Summary

CVE	CVE-2019-12730
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-04 14:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	aa_read_header in libavformat/aadec.c in FFmpeg before 3.2.14 and 4.x before 4.1.4 does not check for sscanf failure and

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
avformat/aadec: Check for scanf() failure · FFmpeg/FFmpeg@ed188f6 · GitHub	MISC	github.com	Patch, Third Party A
Comparing a97ea53...ba11e40 · FFmpeg/FFmpeg · GitHub	MISC	github.com	Third Party Advisor
Bugtraq: [SECURITY] [DSA 4502-1] ffmpeg security update	BUGTRAQ	seclists.org	
USN-4431-1: FFmpeg vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
FFmpeg CVE-2019-12730 Security Bypass Vulnerability	BID	www.securityfocus.com	
Debian -- Security Information -- DSA-4502-1 ffmpeg	DEBIAN	www.debian.org	
git.ffmpeg.org Git - ffmpeg.git/shortlog	CONFIRM	git.ffmpeg.org	
FFmpeg: Multiple vulnerabilities (GLSA 202003-65) — Gentoo security	GENTOO	security.gentoo.org	
git.ffmpeg.org Git - ffmpeg.git/commit	CONFIRM	git.ffmpeg.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 500906 Alpine Linux Security Update for ffmpeg
- 502276 Alpine Linux Security Update for ffmpeg4
- 504749 Alpine Linux Security Update for ffmpeg
- 504767 Alpine Linux Security Update for ffmpeg4