



CVE-2017-14222

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-14222
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-09 01:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In libavformat/mov.c in FFmpeg 3.3.3, a DoS in read_tfra() due to lack of an EOF (End of File) check might cause huge CP

Risk And Classification

Problem Types: CWE-834

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	3.3.3	All	All	All
Application	Ffmpeg	Ffmpeg	3.3.3	All	All	All

References

Reference	Source	Link	Tags
avformat/mov: Fix DoS in read_tfra() · FFmpeg/FFmpeg@9cb4eb7 · GitHub	CONFIRM	github.com	Issue Tracking, Patch, T
Debian -- Security Information -- DSA-3996-1 ffmpeg	DEBIAN	www.debian.org	
FFmpeg 'libavformat/mov.c' Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VI
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

[500897](#) Alpine Linux Security Update for ffmpeg

[502267](#) Alpine Linux Security Update for ffmpeg4

[504740](#) Alpine Linux Security Update for ffmpeg

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)