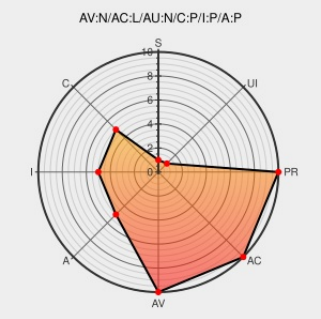
CVE-2015-6823

Published on: 09/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6823

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ffmpeg from Ffmpeg contain the following vulnerability:

The allocate_buffers function in libavcodec/alac.c in FFmpeg before 2.7.2 does not initialize certain context data, which allows remote attackers to cause a denial of service (segmentation violation) or possibly have unspecified other impact via crafted Apple Lossless Audio Codec (ALAC) data.

CVE-2015-6823 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
FFmpeg Security	ffmpeg.org text/html	CONFIRM ffmpeg.org/security.html
FFmpeg Multiple Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1033483
[SECURITY] [DLA 1611-2] libav security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20181221 [SECURITY] [DLA 1611-2] libav security update
git.videolan.org Git - ffmpeg.git/commit	git.videolan.org text/xml	CONFIRM git.videolan.org/?p=ffmpeg.git;a=commit;h=f7068bf277a37479aecde2832208d820682b35e6

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:ffmpeg:ffmpeg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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