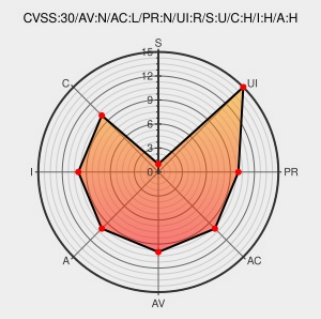
CVE-2018-5684

Published on: 01/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5684

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



Certain versions of Libav from Libav contain the following vulnerability:

In Libav through 12.2, there is an invalid memcpy call in the ff_mov_read_stsd_entries function of libavformat/mov.c. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) and program failure with a crafted avi file.

CVE-2018-5684 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Bug 1110 – Invalid memcpy in ff_mov_read_stsd_entries (libavformat/mov.c)	Exploit, Issue Tracking, Third Party Advisory, bugzilla.libav.org, text/html	MISC bugzilla.libav.org/show_bug.cgi?id=1110

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	Libav	Libav	All	All	All	All

cpe:2.3:a:libav:libav:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→