

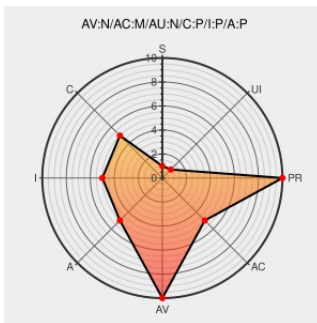


CVE-2015-8364

Published on: 11/26/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8364

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Integer overflow in the ff_ivi_init_planes function in libavcodec/ivi.c in FFmpeg before 2.6.5, 2.7.x before 2.7.3, and 2.8.x through 2.8.2 allows remote attackers to cause a denial of service (out-of-bounds heap-memory access) or possibly have unspecified other impact via crafted image dimensions in Indeo Video Interactive data.

CVE-2015-8364 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 1611-1] libav security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20181220 [SECURITY] [DLA 1611-1] libav security update
openSUSE-SU-2015:2370-1: moderate: Security update for ffmpeg	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2370
USN-2944-1: Libav vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2944-1
git.videolan.org Git - ffmpeg.git/commit	Vendor Advisory git.videolan.org text/xml	CONFIRM git.videolan.org/?p=ffmpeg.git;a=commit;h=df91aa034b82b77a3c4e01791f4a2b2ff6c82066

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
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Application	Ffmpeg	Ffmpeg	2.6.4	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.0	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.2	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.0	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.2	All	All	All
Application	Ffmpeg	Ffmpeg	2.6.4	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.0	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.7.2	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.0	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.1	All	All	All
Application	Ffmpeg	Ffmpeg	2.8.2	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:a:ffmpeg:ffmpeg:2.6.4:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.7.0:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.7.1:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.7.2:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.8.0:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.8.1:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.8.2:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:2.6.4:*****:						

cpe:2.3:a:ffmpeg:ffmpeg:2.7.0:*:*:*:*:*:	
cpe:2.3:a:ffmpeg:ffmpeg:2.7.1:*:*:*:*:*:	
cpe:2.3:a:ffmpeg:ffmpeg:2.7.2:*:*:*:*:*:	
cpe:2.3:a:ffmpeg:ffmpeg:2.8.0:*:*:*:*:*:	
cpe:2.3:a:ffmpeg:ffmpeg:2.8.1:*:*:*:*:*:	
cpe:2.3:a:ffmpeg:ffmpeg:2.8.2:*:*:*:*:*:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→