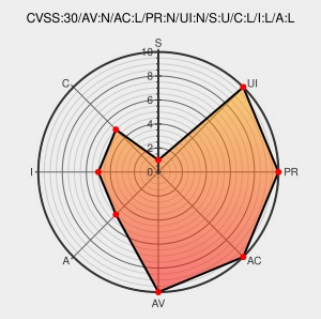
CVE-2015-8662

Published on: 12/23/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-8662

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



Certain versions of Ffmpeg from Ffmpeg contain the following vulnerability:

The ff_dwt_decode function in libavcodec/jpeg2000dwt.c in FFmpeg before 2.8.4 does not validate the number of decomposition levels before proceeding with Discrete Wavelet Transform decoding, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data.

CVE-2015-8662 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

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

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
[SECURITY] [DLA 1611-1] libav security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20181220 [SECURITY] [DLA 1611-1] libav security update

[security-announce] openSUSE-SU-2016:0089-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0089
git.videolan.org Git - ffmpeg.git/commit	git.videolan.org text/xml	CONFIRM git.videolan.org/?p=ffmpeg.git;a=commit;h=75422280fbcdfbe9dc56bde5525b4d8b280f1bc5
FFmpeg Array Access Errors Let Remote Users Cause the Target Application to Crash - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034539

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→