



CVE-2017-17081

Published on: 11/30/2017 12:00:00 AM UTC

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

CVE-2017-17081

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

Certain versions of [Ffmpeg](#) from [Ffmpeg](#) contain the following vulnerability:

The `gmc_mmx` function in `libavcodec/x86/mpegvideodsp.c` in FFmpeg 2.3 and 3.4 does not properly validate widths and heights, which allows remote attackers to cause a denial of service (integer signedness error and out-of-array read) via a crafted MPEG file.

CVE-2017-17081 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
3516 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	Issue Tracking bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=3516#c1
avcodec/x86/mpegvideodsp:	github.com	CONFIRM

Fix signedness bug in need_emu · FFmpeg/FFmpeg@27f8d38 · GitHub

text/html

github.com/FFmpeg/FFmpeg/commit/27f8d386829689c346ff0cef00d3af57b9fb8903

[FFmpeg-devel] [PATCH] avcodec/x86/mpegvideodsp: Fix signedness bug in need_emu

Issue Tracking Patch lists.ffmpeg.org text/x-diff

MISC lists.ffmpeg.org/pipermail/ffmpeg-devel/2017-November/219748.html

avcodec/x86/mpegvideodsp: Fix signedness bug in need_emu · FFmpeg/FFmpeg@58cf31c · GitHub

Patch Vendor Advisory github.com text/html

MISC github.com/FFmpeg/FFmpeg/commit/58cf31cee7a456057f337b3102a03206d833d5e8

Debian -- Security Information -- DSA-4099-1 ffmpeg

www.debian.org Deprecated Link text/html

DEBIAN DSA-4099

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	Ffmpeg	Ffmpeg	3.4	All	All	All
Application	Ffmpeg	Ffmpeg	3.4	All	All	All
cpe:2.3:a:ffmpeg:ffmpeg:3.4:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:3.4:*****:						

No vendor comments have been submitted for this CVE