



CVE-2018-13305

Published on: 07/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:29 PM UTC

CVE-2018-13305

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H



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

In FFmpeg 4.0.1, due to a missing check for negative values of the mquant variable, the vc1_put_blocks_clamped function in libavcodec/vc1_block.c may trigger an out-of-array access while converting a crafted AVI file to MPEG4, leading to an information disclosure or a denial of service.

CVE-2018-13305 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:0024-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0024

avcodec/vc1_block: Fix
mqaunt check for negative
values ·
FFmpeg/FFmpeg@d08d4a8 ·
GitHub

Patch
github.com
text/html

MISC
github.com/FFmpeg/FFmpeg/commit/d08d4a8c7387e758d439b0592782e4cfa2b4d6a4

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.

Related QID Numbers

500903 Alpine Linux Security Update for ffmpeg
502273 Alpine Linux Security Update for ffmpeg4

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	4.0.1	All	All	All
Application	Ffmpeg	Ffmpeg	4.0.1	All	All	All
cpe:2.3:a:ffmpeg:ffmpeg:4.0.1:*:*:*:*:*:						
cpe:2.3:a:ffmpeg:ffmpeg:4.0.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→