



CVE-2017-1000460

Published on: 01/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

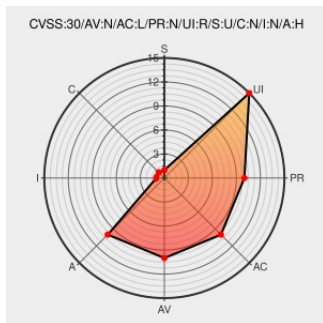
CVE-2017-1000460

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

In line libavcodec/h264dec.c:500 in libav(v13_dev0), ffmpeg(n3.4), chromium(56 prior Feb 13, 2017), the return value of init_get_bits is ignored and get_ue_golomb(&gb) is called on an uninitialized get_bits context, which causes a NULL deref exception.

CVE-2017-1000460 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
Bug 952 – NULL dereference in libavcodec/h264dec.c:499/500	Exploit Issue Tracking Third Party Advisory bugzilla.libav.org text/html	MISC bugzilla.libav.org/show_bug.cgi?id=952

8e313ca08800178efce00045e07dc494d437b70c
- chromium/third_party/ffmpeg - Git at Google

Issue Tracking

Patch

chromium.googlesource.com

text/html

MISC

chromium.googlesource.com/chromium/third_party/ffmpeg/+

[SECURITY] [DLA 1740-1] libav security update

lists.debian.org

text/html

MLIST [debian-lts-announce] 20190330 [SECURITY] [DL

[FFmpeg-cvslog] h264dec: handle zero-sized NAL units in get_last_needed_nal()

Issue Tracking

Patch

lists.ffmpeg.org

text/x-diff

MISC

lists.ffmpeg.org/pipermail/ffmpeg-cvslog/2017-Janu

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
Application	Google	Chrome	All	All	All	All
Application	Libav	Libav	13_dev0	All	All	All
Application	Libav	Libav	13_dev0	All	All	All
cpe:2.3:a:ffmpeg:ffmpeg:3.4:*****:						
cpe:2.3:a:ffmpeg:ffmpeg:3.4:*****:						
cpe:2.3:a:google:chrome:*****:						
cpe:2.3:a:libav:libav:13_dev0:*****:						
cpe:2.3:a:libav:libav:13_dev0:*****:						

No vendor comments have been submitted for this CVE

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report