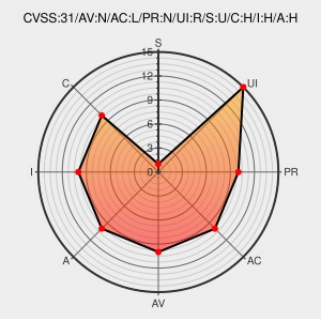
CVE-2020-14212

Published on: 06/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-14212

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



Certain versions of Ffmpeg from Ffmpeg contain the following vulnerability:

FFmpeg through 4.3 has a heap-based buffer overflow in avio_get_str in libavformat/aviobuf.c because dnn_backend_native.c calls ff_dnn_load_model_native and a certain index check is omitted.

CVE-2020-14212 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
#8716 (Heap buffer overflow in ff_dnn_load_model_native) – FFmpeg	Patch, Vendor Advisory, trac.ffmpeg.org, text/html	MISC trac.ffmpeg.org/ticket/8716

FFmpeg - Patchwork	Not Applicable Vendor Advisory patchwork.ffmpeg.org text/html	MISC patchwork.ffmpeg.org/project/ffmpeg/list/?series=1463
FFmpeg: Multiple vulnerabilities (GLSA 202007-58) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-202007-58

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

500910 Alpine Linux Security Update for ffmpeg

502280 Alpine Linux Security Update for ffmpeg4

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	All	All	All	All
Application	Ffmpeg	Ffmpeg	All	All	All	All

cpe:2.3:a:ffmpeg:ffmpeg:*:*:*:*:*:*:*:*:

cpe:2.3:a:ffmpeg:ffmpeg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→