



CVE-2020-20891

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-20891
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-20 16:15:00 UTC
Updated	2021-09-24 21:49:00 UTC
Description	Buffer Overflow vulnerability in function config_input in libavfilter/vf_gblur.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service (DoS) by sending a crafted request to the vulnerable component.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	4.2.1	All	All	All

References

Reference	Source	Link	Tags
git.ffmpeg.org Git - ffmpeg.git/commit	MISC	git.ffmpeg.org	
#8282 (invalid free at libavfilter/avfilter.c:771) – FFmpeg	MISC	trac.ffmpeg.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[751277](#) OpenSUSE Security Update for ffmpeg (openSUSE-SU-2021:3521-1)

[753502](#) SUSE Enterprise Linux Security Update for ffmpeg (SUSE-SU-2023:0005-1)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)