



CVE-2020-22024

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-22024
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-26 21:15:00 UTC
Updated	2021-06-03 12:33:00 UTC
Description	Buffer Overflow vulnerability in FFmpeg 4.2 at the lagfun_frame16 function in libavfilter/vf_lagfun.c, which could let a remote

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	-	All	All

References

Reference	Source	Link	Tags
#8310 (heap-buffer-overflow at libavfilter/vf_lagfun.c:141) – 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

[180785](#) Debian Security Update for ffmpeg (CVE-2020-22024)

[199827](#) Ubuntu Security Notification for FFmpeg Vulnerabilities (USN-6430-1)

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](#)