



# CVE-2020-22051

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

## Summary

<b>CVE</b>	CVE-2020-22051
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-02 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:19:00 UTC
<b>Description</b>	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the filter_frame function in vf_tile.c.

## Risk And Classification

**Problem Types:** CWE-401

## 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
git.videolan.org Git - ffmpeg.git/commitdiff	MISC	<a href="https://git.videolan.org">git.videolan.org</a>	
#8313 (memory leaks in filter_frame()) – FFmpeg	MISC	<a href="https://trac.ffmpeg.org">trac.ffmpeg.org</a>	
git.videolan.org Git - ffmpeg.git/commitdiff		<a href="https://git.videolan.org">git.videolan.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

180735 Debian Security Update for ffmpeg (CVE-2020-22051)

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)**