



CVE-2014-125020

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

Summary

CVE	CVE-2014-125020
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-19 06:15:00 UTC
Updated	2023-11-07 02:18:00 UTC
Description	A vulnerability has been found in FFmpeg 2.0 and classified as critical. This vulnerability affects the function decode_update

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ffmpeg	Ffmpeg	2.0	All	All	All

References

Reference	
CVE-2014-125020 FFmpeg decode_update_thread_context memory corruption (XFDB-91078 / ffmpeg-decodeupdatethread-code-exec)	N
git.videolan.org Git - ffmpeg.git/commit	N
git.videolan.org Git	
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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