



CVE-2019-19721

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

Summary

CVE	CVE-2019-19721
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-15 18:15:00 UTC
Updated	2023-11-07 03:07:00 UTC
Description	An off-by-one error in the DecodeBlock function in codec/sdl_image.c in VideoLAN VLC media player before 3.0.9 allows re

Risk And Classification

Problem Types: CWE-787 | CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	All	All	All	All
Application	Videolan	Vlc Media Player	All	All	All	All

References

Reference	Source	Li
git.videolan.org Git - vlc/vlc-3.0.git/commit		git
GitHub - libsdl-org/SDL_image: Image decoding for many popular formats for Simple Directmedia Layer.	MISC	hg
721940 - (CVE-2019-19721, VideoLAN-SB-VLC-309) <media-video/vlc-3.0.10: out of bound read (VideoLAN-SB-VLC-309)	MISC	bu
VideoLAN Security Advisories	MISC	wv
git.videolan.org Git - vlc/vlc-3.0.git/commit	MISC	git
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199556](#) Ubuntu Security Notification for VLC media player Vulnerabilities (USN-6180-1)

501270 Alpine Linux Security Update for vlc

505489 Alpine Linux Security Update for vlc

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)