



CVE-2008-2147

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

Summary

CVE	CVE-2008-2147
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-12 20:20:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	Untrusted search path vulnerability in VideoLAN VLC before 0.9.0 allows local users to execute arbitrary code via a malicious

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc	0.4.6	All	All	All
Application	Videolan	Vlc	0.5.0	All	All	All
Application	Videolan	Vlc	0.5.1	All	All	All
Application	Videolan	Vlc	0.5.1a	All	All	All
Application	Videolan	Vlc	0.5.2	All	All	All
Application	Videolan	Vlc	0.5.3	All	All	All
Application	Videolan	Vlc	0.6.0	All	All	All
Application	Videolan	Vlc	0.6.1	All	All	All
Application	Videolan	Vlc	0.6.2	All	All	All
Application	Videolan	Vlc	0.7.0	All	All	All
Application	Videolan	Vlc	0.7.1	All	All	All
Application	Videolan	Vlc	0.7.2	All	All	All
Application	Videolan	Vlc	0.8.0	All	All	All
Application	Videolan	Vlc	0.8.1	All	All	All
Application	Videolan	Vlc	0.8.2	All	All	All
Application	Videolan	Vlc	0.8.4	All	All	All
Application	Videolan	Vlc	0.8.4a	All	All	All

Application	Videolan	Vlc	0.8.5	All	All	All
Application	Videolan	Vlc	0.8.6a	All	All	All
Application	Videolan	Vlc	0.8.6b	All	All	All
Application	Videolan	Vlc	0.8.6c	All	All	All
Application	Videolan	Vlc	0.8.6d	All	All	All
Application	Videolan	Vlc	0.8.6e	All	All	All
Application	Videolan	Vlc	All	All	All	All
Application	Videolan	Vlc	0.4.6	All	All	All
Application	Videolan	Vlc	0.5.0	All	All	All
Application	Videolan	Vlc	0.5.1	All	All	All
Application	Videolan	Vlc	0.5.1a	All	All	All
Application	Videolan	Vlc	0.5.2	All	All	All
Application	Videolan	Vlc	0.5.3	All	All	All
Application	Videolan	Vlc	0.6.0	All	All	All
Application	Videolan	Vlc	0.6.1	All	All	All
Application	Videolan	Vlc	0.6.2	All	All	All
Application	Videolan	Vlc	0.7.0	All	All	All
Application	Videolan	Vlc	0.7.1	All	All	All
Application	Videolan	Vlc	0.7.2	All	All	All
Application	Videolan	Vlc	0.8.0	All	All	All
Application	Videolan	Vlc	0.8.1	All	All	All
Application	Videolan	Vlc	0.8.2	All	All	All
Application	Videolan	Vlc	0.8.4	All	All	All
Application	Videolan	Vlc	0.8.4a	All	All	All
Application	Videolan	Vlc	0.8.5	All	All	All
Application	Videolan	Vlc	0.8.6a	All	All	All
Application	Videolan	Vlc	0.8.6b	All	All	All
Application	Videolan	Vlc	0.8.6c	All	All	All
Application	Videolan	Vlc	0.8.6d	All	All	All
Application	Videolan	Vlc	0.8.6e	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
#1578 (VLC executes arbitrary plugins) - VLC - Trac	CONFIRM	trac.videolan.org	

git.videolan.org Git			git.videolan.org	
git.videolan.org Git - vlc.git/commit	CONFIRM		git.videolan.org	
Gentoo update for vlc - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA		secunia.com	
Gentoo Linux Documentation -- VLC: Multiple vulnerabilities	GENTOO		security.gentoo.org	
CVE Program record	CVE.ORG		www.cve.org	canonic
NVD vulnerability detail	NVD		nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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