



CVE-2014-9598

Published on: 01/21/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9598

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Vlc Media Player](#) from [Videolan](#) contain the following vulnerability:

The picture_Release function in misc/picture.c in VideoLAN VLC media player 2.1.5 allows remote attackers to execute arbitrary code or cause a denial of service (write access violation) via a crafted M2V file.

CVE-2014-9598 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Full Disclosure: VLC Media Player 2.1.5 Memory Corruption Vulnerabilities (CVE-2014-9597, CVE-2014-9598)

[seclists.org](#)
[text/html](#)

[FULLDISC 20150116 VLC Media Player 2.1.5 Memory Corruption Vulnerabilities \(CVE-2014-9597, CVE-2014-9598\)](#)

#13390 (VLC Player 2.1.5 Write Access Violation Vulnerability) – VLC

[trac.videolan.org](#)
[text/html](#)

[MISC trac.videolan.org/vlc/ticket/13390](#)

VLC: Multiple vulnerabilities (GLSA 201603-08) — Gentoo Security

[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-201603-08](#)

Binary Sniper: VLC Media Player 2.1.5 Memory Corruption Vulnerabilities

[www.binarysniper.net](#)
[text/html](#)

[MISC www.binarysniper.net/2015/01/vlc-media-player-215-memory-corruption.html](#)

windbglog.txt on Ticket #13390 – Attachment – VLC

[trac.videolan.org](#)
[text/html](#)

[MISC trac.videolan.org/vlc/attachment/ticket/13390/windbglog.txt](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Videolan	Vlc Media Player	2.1.5	All	All	All
Application	Videolan	Vlc Media Player	2.1.5	All	All	All
cpe:2.3:a:videolan:vlc_media_player:2.1.5:*:*:*:*:*:						
cpe:2.3:a:videolan:vlc_media_player:2.1.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)