



CVE-2014-9626

Published on: 01/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9626

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Integer underflow in the MP4_ReadBox_String function in modules/demux/mp4/libmp4.c in VideoLAN VLC media player before 2.1.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a box size less than 7.

CVE-2014-9626 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

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
oss-security - Vulnerabilities in VLC 2.1.5	Mailing List Patch Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2015/01/20/5

VideoLAN - VideoLAN Security Advisory 1501

Vendor Advisory

www.videolan.org

text/xml

 **CONFIRM** www.videolan.org/security/sa1501.html

demux: mp4: fix buffer overflow in parsing of string boxes. · videolan/vlc@2e7c709 · GitHub

Patch

Third Party Advisory

github.com

text/html

 **MISC**
github.com/videolan/vlc/commit/2e7c7091a61aa5d07e7997b393d821e91f593c39

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	All	All	All	All
Application	Videolan	Vlc Media Player	All	All	All	All

cpe:2.3:a:videolan:vlc_media_player:*****:

cpe:2.3:a:videolan:vlc_media_player:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →