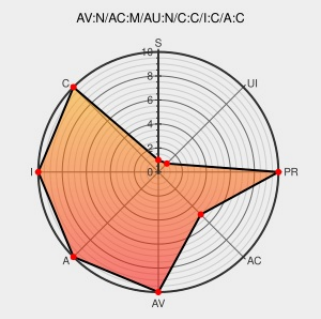
CVE-2011-3625

Published on: 06/11/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:14 PM UTC

CVE-2011-3625

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mplayer2 from Mplayer2 contain the following vulnerability:

Stack-based buffer overflow in the sub_read_line_sami function in subreader.c in MPlayer, as used in SMPlayer 0.6.9, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string in a SAMI subtitle file.

CVE-2011-3625 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisory SA55486 - Gentoo update for MPlayer - Secunia	web.archive.org text/html	SECUNIA 55486
	Vendor Advisory labs.mwrinfosecurity.com application/pdf	MISC labs.mwrinfosecurity.com/system/assets/149/original/mwri_mplayer-sami-subtitles_2011-08-12.pdf
oss-security - Re: CVE request: mplayer SAMI subtitle parsing buffer overflow	www.openwall.com text/html	MLIST [oss-security] 20111018 Re: CVE request: mplayer SAMI subtitle parsing buffer overflow
Gentoo Linux Documentation -- MPlayer: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201310-13
No Description Provided	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM git.mplayer2.org/mplayer2/commit/?id=27b88a09c5319deb62221b8cd0ecc14cd1136e4a

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	Mplayer2	Mplayer2	-	All	All	All
Application	Mplayer2	Mplayer2	-	All	All	All
Application	Ricardo Villalba	Smplayer	0.6.9	All	All	All
Application	Ricardo Villalba	Smplayer	0.6.9	All	All	All

cpe:2.3:a:mplayer2:mplayer2:-:*:*:*:*:*:*:*:

cpe:2.3:a:mplayer2:mplayer2:-:*:*:*:*:*:*:*:

cpe:2.3:a:ricardo_villalba:smplayer:0.6.9:*:*:*:*:*:*:*:

cpe:2.3:a:ricardo_villalba:smplayer:0.6.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→