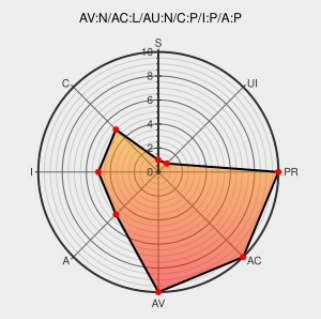
CVE-2005-1195

Published on: 04/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1195

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



Certain versions of Mplayer from Mplayer contain the following vulnerability:

Multiple heap-based buffer overflows in the code used to handle (1) MMS over TCP (MMST) streams or (2) RealMedia RTSP streams in xine-lib before 1.0, and other products that use xine-lib such as MPlayer 1.0pre6 and earlier, allow remote malicious servers to execute arbitrary code.

CVE-2005-1195 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityTracker.com Archives - MPlayer MMST and RTSP Buffer Overflows Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1013771
No Description Provided	cvs.sourceforge.net Inactive Link Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/librtsp/rtsp.c?r1=1.18&r2=1.19&diff_format=u
404 Not Found	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM www.mplayerhq.hu/homepage/design7/news.html#vuln10
MPlayer MMST Stream ID Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 13271

SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20050421 [PLSN-0003] - Remote exploits in MPlayer
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 15711
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mplayer-mmst-stream-bo(20175)
Bugtraq: xine security announcement: multiple heap overflows in MMS and Real RTSP streaming clients	seclists.org text/html	BUGTRAQ 20050421 xine security announcement: multiple heap overflows in MMS and Real RTSP streaming clients
404 Not Found	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM www.mplayerhq.hu/homepage/design7/news.html#vuln11
	cvs.sourceforge.net text/x-diff Inactive Link Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/mms.c?r1=1.55&r2=1.56&diff_format=u
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 15712
Secunia - Advisories - MPlayer RTSP and MMST Streams Buffer Overflow Vulnerabilities	Patch web.archive.org text/html	SECUNIA 15014
Gentoo Linux Documentation -- MPlayer: Two heap overflow vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200504-19
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mplayer-rtsp-stream-bo(20171)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mplayer	Mplayer	All	All	All	All
Application	Xine	Xine-lib	1_beta1	All	All	All
Application	Xine	Xine-lib	1_beta10	All	All	All
Application	Xine	Xine-lib	1_beta11	All	All	All
Application	Xine	Xine-lib	1_beta2	All	All	All
Application	Xine	Xine-lib	1_beta3	All	All	All
Application	Xine	Xine-lib	1_beta4	All	All	All
Application	Xine	Xine-lib	1_beta5	All	All	All

Application	Xine	Xine-lib	1_beta6	All	All	All
Application	Xine	Xine-lib	1_beta7	All	All	All
Application	Xine	Xine-lib	1_beta8	All	All	All
Application	Xine	Xine-lib	1_beta9	All	All	All
Application	Xine	Xine-lib	1_rc2	All	All	All
Application	Xine	Xine-lib	1_rc3a	All	All	All
Application	Xine	Xine-lib	1_rc3b	All	All	All
Application	Xine	Xine-lib	1_rc3c	All	All	All
Application	Xine	Xine-lib	1_beta1	All	All	All
Application	Xine	Xine-lib	1_beta10	All	All	All
Application	Xine	Xine-lib	1_beta11	All	All	All
Application	Xine	Xine-lib	1_beta2	All	All	All
Application	Xine	Xine-lib	1_beta3	All	All	All
Application	Xine	Xine-lib	1_beta4	All	All	All
Application	Xine	Xine-lib	1_beta5	All	All	All
Application	Xine	Xine-lib	1_beta6	All	All	All
Application	Xine	Xine-lib	1_beta7	All	All	All
Application	Xine	Xine-lib	1_beta8	All	All	All
Application	Xine	Xine-lib	1_beta9	All	All	All
Application	Xine	Xine-lib	1_rc2	All	All	All
Application	Xine	Xine-lib	1_rc3a	All	All	All
Application	Xine	Xine-lib	1_rc3b	All	All	All
Application	Xine	Xine-lib	1_rc3c	All	All	All

cpe:2.3:a:mplayer:mplayer:*:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta10:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta11:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta4:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta6:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta7:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta8:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta9:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3a:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3b:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3c:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta10:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta11:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta4:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta6:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta7:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta8:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_beta9:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3a:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3b:*:*:*:*:*:*:*:

cpe:2.3:a:xine:xine-lib:1_rc3c:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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