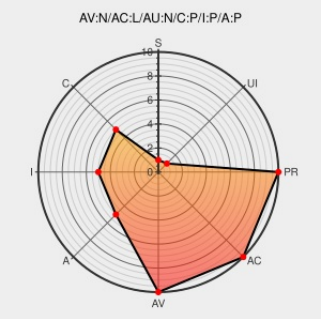
CVE-2002-1321

Published on: 11/27/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1321

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



Certain versions of Realone Player from Realnetworks contain the following vulnerability:

Multiple buffer overflows in RealOne and RealPlayer allow remote attackers to execute arbitrary code via (1) a Synchronized Multimedia Integration Language (SMIL) file with a long parameter, (2) a long long filename in a rtsp:// request, e.g. from a .m3u file, or (3) certain "Now Playing" options on a downloaded file with a long filename.

CVE-2002-1321 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF realplayer-rtsp-filename-bo(10677)
RealOne Player SMIL File Heap Corruption Vulnerability	cve.report (archive) text/html	BID 6227
RealPlayer Long File Name Now Playing Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 6229
'Mulitple Buffer Overflow conditions in RealPlayer/RealOne (#NISR22112002)' - MARC	marc.info text/html	BUGTRAQ 20021122 Mulitple Buffer Overflow conditions in RealPlayer/RealOne (#NISR22112002)
RealNetworks Support	service.real.com text/html	CONFIRM service.real.com/help/faq/security/bufferoverrun_player.html

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	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realplayer	All	g2	All	All
Application	Realnetworks	Realplayer	6.0	All	win32	All
Application	Realnetworks	Realplayer	7.0	All	win32	All
Application	Realnetworks	Realplayer	8.0	All	win32	All
Application	Realnetworks	Realplayer	All	g2	All	All
Application	Realnetworks	Realplayer	6.0	All	win32	All
Application	Realnetworks	Realplayer	7.0	All	win32	All
Application	Realnetworks	Realplayer	8.0	All	win32	All

cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:*:g2:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:6.0:*:win32:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:7.0:*:win32:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:8.0:*:win32:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:*:g2:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:6.0:*:win32:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:7.0:*:win32:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:8.0:*:win32:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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