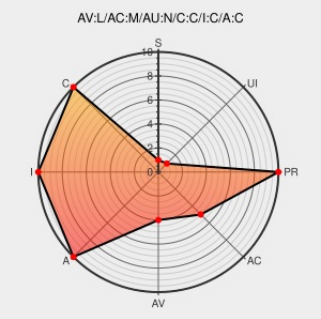
CVE-2010-5228

Published on: 09/07/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:06 PM UTC

CVE-2010-5228

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



Certain versions of Realplayer Sp from Realnetworks contain the following vulnerability:

Untrusted search path vulnerability in RealPlayer SP 1.1.5 12.0.0.879 allows local users to gain privileges via a Trojan horse rio500.dll file in the current working directory, as demonstrated by a directory that contains a .avi file. NOTE: some of these details are obtained from third party information.

CVE-2010-5228 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link
Faculty & Research | Computer Science	www.cs.ucdavis.edu application/pdf	MISC www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-2.pdf
RealPlayer Insecure Library Loading Vulnerability - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 41092

There are currently no OIDs associated with this CVE

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Realplayer Sp	1.1.5	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.5	All	All	All

cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→