



CVE-2010-5228

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

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

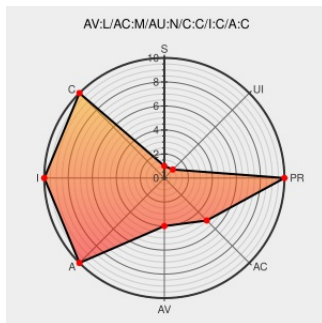
CVE-2010-5228

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 [M](#) 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	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

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 OIDs associated with this CVE

There are currently no CVEs 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→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)