

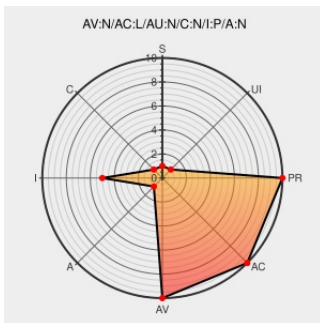


CVE-2005-2055

Published on: 06/28/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2055

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Realone Player](#) from [Realnetworks](#) contain the following vulnerability:

RealPlayer 8, 10, 10.5 (6.0.12.1040-1069), and Enterprise and RealOne Player v1 and v2 allows remote malicious web server to create an arbitrary HTML file that executes an RM file via "default settings of earlier Internet Explorer browsers".

CVE-2005-2055 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Customer Support - Real Security Updates

[Patch](#)

[Vendor Advisory](#)

[service.real.com](#)

[text/html](#)

[CONFIRM service.real.com/help/faq/security/050623_player/EN/](#)

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)

Known/Annotated Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realplayer	All	All	enterprise	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040_1069	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	All	All	enterprise	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040_1069	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
cpe:2.3:a:realnetworks:realone_player:1.0:****:****:						
cpe:2.3:a:realnetworks:realone_player:2.0:****:****:						
cpe:2.3:a:realnetworks:realone_player:1.0:****:****:						
cpe:2.3:a:realnetworks:realone_player:2.0:****:****:						
cpe:2.3:a:realnetworks:realplayer:*:enterprise:****:						
cpe:2.3:a:realnetworks:realplayer:10.0:****:****:						
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1040_1069:****:****:						
cpe:2.3:a:realnetworks:realplayer:8.0:****:****:						
cpe:2.3:a:realnetworks:realplayer:*:enterprise:****:						
cpe:2.3:a:realnetworks:realplayer:10.0:****:****:						
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1040_1069:****:****:						
cpe:2.3:a:realnetworks:realplayer:8.0:****:****:						

No vendor comments have been submitted for this CVE

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](#)