



CVE-2010-4396

Published on: 12/14/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:00 PM UTC

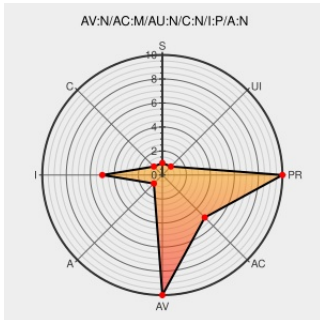
CVE-2010-4396

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-zone scripting vulnerability in the HandleAction method in a certain ActiveX control in RealNetworks RealPlayer 11.0 through 11.1, RealPlayer SP 1.0 through 1.1.5, and RealPlayer Enterprise 2.1.2 allows remote attackers to inject arbitrary web script or HTML in the Local Zone by specifying a local file in a NavigateToURL action, as demonstrated by a local skin file.

CVE-2010-4396 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
RealPlayer and StarSearch by Real Official Homepage — Real.com	Vendor Advisory service.real.com text/html	CONFIRM service.real.com/realplayer/security/12102010_player/en/
SecurityTracker.com Archives - RealPlayer Buffer Overflows and Memory Corruption Errors Let Remote Users Execute Arbitrary Code	www.securitytracker.com text/html	SECTrack 1024861
Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-10-275
No Description Provided	osvdb.org	OSVDB 69855

[Inactive Link](#) [Not Archived](#)

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	Realplayer	11.0	All	All	All
Application	Realnetworks	Realplayer	11.0.1	All	All	All
Application	Realnetworks	Realplayer	11.0.2	All	All	All
Application	Realnetworks	Realplayer	11.0.3	All	All	All
Application	Realnetworks	Realplayer	11.0.4	All	All	All
Application	Realnetworks	Realplayer	11.0.5	All	All	All
Application	Realnetworks	Realplayer	11.1	All	All	All
Application	Realnetworks	Realplayer	2.1.2	All	enterprise	All
Application	Realnetworks	Realplayer	11.0	All	All	All
Application	Realnetworks	Realplayer	11.0.1	All	All	All
Application	Realnetworks	Realplayer	11.0.2	All	All	All
Application	Realnetworks	Realplayer	11.0.3	All	All	All
Application	Realnetworks	Realplayer	11.0.4	All	All	All
Application	Realnetworks	Realplayer	11.0.5	All	All	All
Application	Realnetworks	Realplayer	11.1	All	All	All
Application	Realnetworks	Realplayer	2.1.2	All	enterprise	All
Application	Realnetworks	Realplayer Sp	1.0.0	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.5	All	All	All
Application	Realnetworks	Realplayer Sp	1.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.3	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.4	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.5	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.0	All	All	All

Application	Realnetworks	Realplayer Sp	1.0.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.5	All	All	All
Application	Realnetworks	Realplayer Sp	1.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.3	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.4	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.5	All	All	All
cpe:2.3:a:realnetworks:realplayer:11.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.1:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.2:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.3:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.4:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.5:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.1:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:2.1.2:*:*:enterprise:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.1:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.2:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.3:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.4:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.0.5:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:11.1:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer:2.1.2:*:*:enterprise:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer_sp:1.0.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer_sp:1.0.1:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer_sp:1.0.2:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer_sp:1.0.5:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realplayer_sp:1.1:*:*:*:*:*:						

cpe:2.3:a:realnetworks:realplayer_sp:1.1.1:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.2:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.3:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.4:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.0.0:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.0.1:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.0.2:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.0.5:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.1:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.2:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.3:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.4:*****:
cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)