

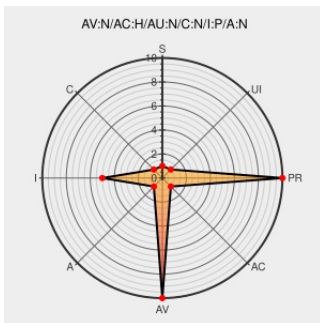


CVE-2005-1695

Published on: 05/24/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1695

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

Certain versions of [Postnuke](#) from [Postnuke Software Foundation](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the RSS module in PostNuke 0.750 and 0.760RC2 and RC3 allow remote attackers to inject arbitrary web script or HTML via the (1) rss_url parameter to magpie_slashbox.php, or the url parameter to (2) magpie_simple.php or (3) magpie_debug.php.

CVE-2005-1695 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

**Access
Vector**

NETWORK

**Access
Complexity**

HIGH

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

PARTIAL

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

'[SECURITYREASON.COM] PostNuke XSS 0.760{RC2,RC3}' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050521 \[SECURITYREASON.COM\] PostNuke XSS 0.760{RC2,RC3}](#)

403 Forbidden

[Patch](#)
[Vendor Advisory](#)
[news.postnuke.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM news.postnuke.com/modules.php?op=modload&name=News&file=article&sid=2691](#)

'[SECURITYREASON.COM] PostNuke XSS and Full path disclosure' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050521 \[SECURITYREASON.COM\] PostNuke XSS and Full path disclosure](#)

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,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postnuke Software Foundation	Postnuke	0.750	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc2	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.750	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc2	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc3	All	All	All
cpe:2.3:a:postnuke_software_foundation:postnuke:0.750:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc2:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc3:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.750:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc2:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)