



CVE-2005-1696

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

Last Modified on: 03/23/2021 11:27:25 PM UTC

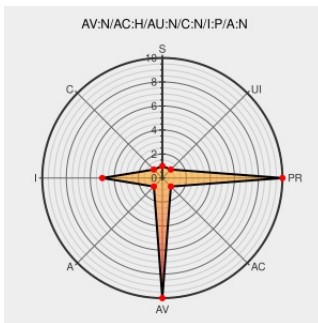
CVE-2005-1696

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 PostNuke 0.750 and 0.760RC3 allow remote attackers to inject arbitrary web script or HTML via the (1) skin or (2) paletteid parameter to demo.php in the Xanthia module, or (3) the serverName parameter to config.php in the Multisites (aka NS-Multisites) module.

CVE-2005-1696 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

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, 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	Postnuke Software Foundation	Postnuke	0.750	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_rc3	All	All	All
cpe:2.3:a:postnuke_software_foundation:postnuke:0.750:*:*:*:*:*:						
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_rc3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)