

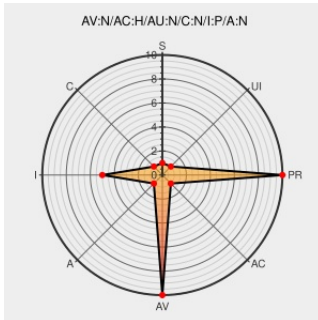


CVE-2005-1049

Published on: 04/12/2005 12:00:00 AM UTC

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

CVE-2005-1049

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

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

Multiple cross-site scripting vulnerabilities in PostNuke 0.760-RC3 allow remote attackers to inject arbitrary web script or HTML via the (1) module parameter to admin.php or (2) op parameter to user.php. NOTE: the vendor reports that certain issues could not be reproduced for 760 RC3, or for .750. However, the op/user.php issue exists when the pnAntiCracker setting is disabled.

CVE-2005-1049 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

PostNuke Phoenix OP Parameter Remote Cross-Site Scripting Vulnerability

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 13075](#)

'Sql injection, xss and path disclosure vulnerabilities in' - MARC

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

[🌐](#) [BUGTRAQ 20050408 Sql injection, xss and path disclosure vulnerabilities in PostNuke 0.760-RC3](#)

Secunia - Advisories - PostNuke Cross-Site Scripting and SQL Injection Vulnerabilities

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 14868](#)

SecurityTracker.com Archives -

[securitytracker.com](#)

[🌐](#) [SECTrack 1013670](#)

Security Machine Room Advisories PostNuke Input Validation Holes in News Module Permits SQL Injection and in 'admin.php' and 'user.php' Permit Cross-Site Scripting Attacks	securitymachineroom.com text/html	SECURITY MACHINEROOM
No Description Provided	digitalparadox.org	MISC digitalparadox.org/advisories/postnuke.txt
	Inactive Link Not Archived	
No Description Provided	Patch cvs.postnuke.com	MISC cvs.postnuke.com/viewcvs.cgi/Historic_PostNuke_Library/postnuke-devel/html/user.php.diff?r1=1.18&r2=1.19
	Inactive Link Not Archived	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF postnuke-adminphp-userphp-xss(20018)
No Description Provided	www.osvdb.org	OSVDB 15370
	Inactive Link Not Archived	
PostNuke Phoenix Module Parameter Remote Cross-Site Scripting Vulnerability	Exploit Patch cve.report (archive) text/html	BID 13076
403 Forbidden	Patch Vendor Advisory news.postnuke.com text/html	MISC news.postnuke.com/modules.php?op=modload&name=News&file=article&sid=2679
	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	Postnuke Software Foundation	Postnuke	0.760_rc3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc3	All	All	All
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc3:*:*:*:*:*:						
cpe:2.3:a:postnuke_software_foundation:postnuke:0.760_rc3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)