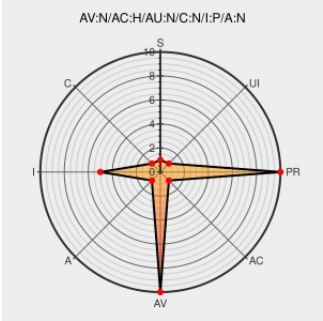
CVE-2005-1049

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	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	SECUNIA 14868
SecurityTracker.com Archives -	securitytracker.com	SECTRACK 1013670

PostNuke Input Validation Holes in News Module Permits SQL Injection and in 'admin.php' and 'user.php' Permit Cross-Site Scripting Attacks	text/html	
No Description Provided	digitalparadox.org Inactive Link Not Archived	MISC digitalparadox.org/advisories/postnuke.txt
No Description Provided	Patch cvs.postnuke.com Inactive Link Not Archived	MISC cvs.postnuke.com/viewcvs.cgi/Historic_PostNuke_Library/postnuke-devel/html/user.php.diff?r1=1.18&r2=1.19
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF postnuke-adminphp-userphp-xss(20018)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 15370
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 Inactive Link Not Archived	MISC news.postnuke.com/modules.php?op=modload&name=News&file=article&sid=2679

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→

CVE.report and Source URL Uptime Status status.cve.report