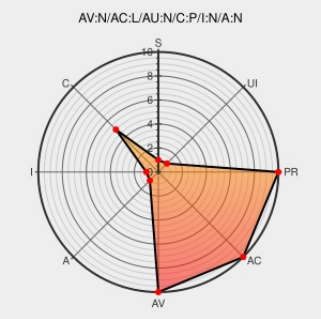
CVE-2005-1621

Published on: 05/16/2005 12:00:00 AM UTC

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

CVE-2005-1621

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Postnuke from Postnuke Software Foundation contain the following vulnerability:

Directory traversal vulnerability in the pnModFunc function in pnMod.php for PostNuke 0.750 through 0.760rc4 allows remote attackers to read arbitrary files via a .. (dot dot) in the func parameter to index.php.

CVE-2005-1621 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
No Description Provided	Patch, cvs.postnuke.com, Inactive Link, Not Archived	CONFIRM cvs.postnuke.com/viewcvs.cgi/Historic_PostNuke_Library/postnuke-devel/html/includes/pnMod.php.diff?r1=1.47&r2=1.48
403 Forbidden	news.postnuke.com, text/html, Inactive Link, Not Archived	CONFIRM news.postnuke.com/Article2690.html
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2005-0553
403 Forbidden	news.postnuke.com, text/html, Inactive Link, Not Archived	CONFIRM news.postnuke.com/modules.php?op=modload&name=News&file=article&sid=2691
'Postnuke 0.750 - 0.760rc4 local file	marc.info	BUGTRAQ 20050516 Postnuke 0.750 - 0.760rc4 local file

inclusion' - MARC	text/html	inclusion

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_rc2	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc4	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
Application	Postnuke Software Foundation	Postnuke	0.760_rc4	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:0.760_rc4:*:*:*:*:*:*:*:

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:0.760_rc4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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