

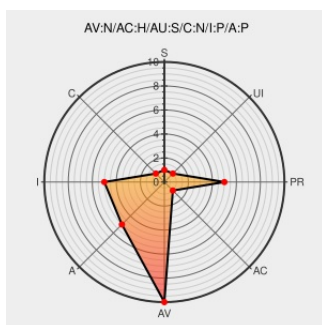


CVE-2006-4759

Published on: 09/13/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

CVE-2006-4759

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

Certain versions of [Punbb](#) from [Punbb](#) contain the following vulnerability:

PunBB 1.2.12 does not properly handle an avatar directory pathname ending in %00, which allows remote authenticated administrative users to upload arbitrary files and execute code, as demonstrated by a query to admin_options.php with an avatars_dir parameter ending in %00.

NOTE: this issue was originally disputed by the vendor, but the dispute was withdrawn on 20060926.

CVE-2006-4759 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.6 - LOW**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060911 ShAnKaR: multiple PHP application poison NULL byte vulnerability](#)

[VIM] Dispute - CVE-2006-4759 - PunBB

www.attrition.org
text/html

[VIM 20060919 Dispute - CVE-2006-4759 - PunBB](#)

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060919 Re: ShAnKaR: multiple PHP application poison NULL byte vulnerability](#)

[VIM] PunBB - more

www.attrition.org
text/html

[VIM 20060925 PunBB - more](#)

уязвимости во многих популярных движках из за некоректной работы файловых функций языка PHP	Exploit www.security.nnov.ru text/html	MISC www.security.nnov.ru/Odocument221.html
[VIM] PunBB - more	www.attrition.org text/html	VIM 20060926 PunBB - more
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CONFIRM forums.punbb.org/viewtopic.php?id=13255
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpbb-nullbyte-file-upload(28884)

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	Punbb	Punbb	1.2.12	All	All	All
Application	Punbb	Punbb	1.2.12	All	All	All
cpe:2.3:a:punbb:punbb:1.2.12:*:*:*:*:*:						
cpe:2.3:a:punbb:punbb:1.2.12:*:*:*:*:*:						

[← Previous ID](#)

[Next ID →](#)