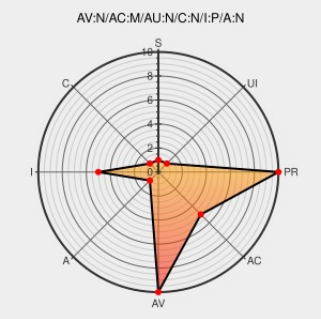
CVE-2006-1089

Published on: 03/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1089

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



Certain versions of Punbb from Punbb contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in header.php in PunBB 1.2.10 allows remote attackers to inject arbitrary web script or HTML via the URL, which is not properly handled when the PHP_SELF variable is used to handle a pun_page tag.

CVE-2006-1089 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
	Patch, www.punbb.org, text/x-diff, Inactive Link, Not Archived	CONFIRM www.punbb.org/download/patch/punbb-1.2.10_to_1.2.11.patch
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-0773
	www.punbb.org, text/plain, Inactive Link, Not Archived	CONFIRM www.punbb.org/changelogs/1.2.10_to_1.2.11.txt
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF punbb-header-xss(24982)
PunBB Header.PHP Cross-Site Scripting Vulnerability	cve.report (archive), text/html	BID 16891

PunBB "header.php" Cross-Site Scripting Vulnerability - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19039

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	1.0	All	All	All
Application	Punbb	Punbb	1.0.1	All	All	All
Application	Punbb	Punbb	1.0_alpha	All	All	All
Application	Punbb	Punbb	1.0_beta1	All	All	All
Application	Punbb	Punbb	1.0_beta1a	All	All	All
Application	Punbb	Punbb	1.0_beta2	All	All	All
Application	Punbb	Punbb	1.0_beta3	All	All	All
Application	Punbb	Punbb	1.0_rc1	All	All	All
Application	Punbb	Punbb	1.0_rc2	All	All	All
Application	Punbb	Punbb	1.1	All	All	All
Application	Punbb	Punbb	1.1.1	All	All	All
Application	Punbb	Punbb	1.1.2	All	All	All
Application	Punbb	Punbb	1.1.3	All	All	All
Application	Punbb	Punbb	1.1.4	All	All	All
Application	Punbb	Punbb	1.1.5	All	All	All
Application	Punbb	Punbb	1.2	All	All	All
Application	Punbb	Punbb	1.2.1	All	All	All
Application	Punbb	Punbb	1.2.10	All	All	All
Application	Punbb	Punbb	1.2.2	All	All	All
Application	Punbb	Punbb	1.2.3	All	All	All
Application	Punbb	Punbb	1.2.4	All	All	All
Application	Punbb	Punbb	1.2.5	All	All	All
Application	Punbb	Punbb	1.2.6	All	All	All
Application	Punbb	Punbb	1.2.7	All	All	All
Application	Punbb	Punbb	1.2.8	All	All	All

Application	Punbb	Punbb	1.2.9	All	All	All
Application	Punbb	Punbb	1.0	All	All	All
Application	Punbb	Punbb	1.0.1	All	All	All
Application	Punbb	Punbb	1.0_alpha	All	All	All
Application	Punbb	Punbb	1.0_beta1	All	All	All
Application	Punbb	Punbb	1.0_beta1a	All	All	All
Application	Punbb	Punbb	1.0_beta2	All	All	All
Application	Punbb	Punbb	1.0_beta3	All	All	All
Application	Punbb	Punbb	1.0_rc1	All	All	All
Application	Punbb	Punbb	1.0_rc2	All	All	All
Application	Punbb	Punbb	1.1	All	All	All
Application	Punbb	Punbb	1.1.1	All	All	All
Application	Punbb	Punbb	1.1.2	All	All	All
Application	Punbb	Punbb	1.1.3	All	All	All
Application	Punbb	Punbb	1.1.4	All	All	All
Application	Punbb	Punbb	1.1.5	All	All	All
Application	Punbb	Punbb	1.2	All	All	All
Application	Punbb	Punbb	1.2.1	All	All	All
Application	Punbb	Punbb	1.2.10	All	All	All
Application	Punbb	Punbb	1.2.2	All	All	All
Application	Punbb	Punbb	1.2.3	All	All	All
Application	Punbb	Punbb	1.2.4	All	All	All
Application	Punbb	Punbb	1.2.5	All	All	All
Application	Punbb	Punbb	1.2.6	All	All	All
Application	Punbb	Punbb	1.2.7	All	All	All
Application	Punbb	Punbb	1.2.8	All	All	All
Application	Punbb	Punbb	1.2.9	All	All	All

cpe:2.3:a:punbb:punbb:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_alpha:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta1a:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_alpha:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta1a:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.0_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→