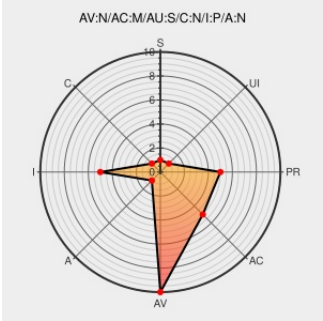
CVE-2005-3310

Published on: 10/25/2005 12:00:00 AM UTC

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

CVE-2005-3310

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



Certain versions of Phpbb from Phpbb Group contain the following vulnerability:

Interpretation conflict in phpBB 2.0.17, with remote avatars and avatar uploading enabled, allows remote authenticated users to inject arbitrary web script or HTML via an HTML file with a GIF or JPEG file extension, which causes the HTML to be executed by a victim who views the file in Internet Explorer, which renders malformed image types as HTML, enabling cross-site scripting (XSS) attacks. NOTE: it could be argued that this vulnerability is due to a design flaw in Internet Explorer (CVE-2005-3312) and the proper fix should be in that browser; if so, then this should not be treated as a vulnerability in phpBB.

CVE-2005-3310 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Neohapsis Archives - Full Disclosure List - #0479 - [Full-disclosure] phpBB 2.0.17 (and other BB systems as well) Cookie disclosure exploit.	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20051022 phpBB 2.0.17 (and other BB systems as well) Cookie disclosure exploit.
Debian -- Security Information -- DSA-925-1 phpbb2	Patch, Vendor Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-925

Secunia - Advisories - phpBB Avatar Script Insertion Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17295
Secunia - Advisories - Debian update for phpbb2	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18098
'phpBB 2.0.17 (and other BB systems as well) Cookie disclosure' - MARC	marc.info text/html	BUGTRAQ 20051022 phpBB 2.0.17 (and other BB systems as well) Cookie disclosure
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpbb-avatar-bypass-security(22837)
phpBB Avatar Upload HTML Injection Vulnerability	cve.report (archive) text/html	BID 15170

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	Phpbb Group	Phpbb	2.0.17	All	All	All
Application	Phpbb Group	Phpbb	2.0.17	All	All	All

cpe:2.3:a:phpbb_group:phpbb:2.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.17:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→