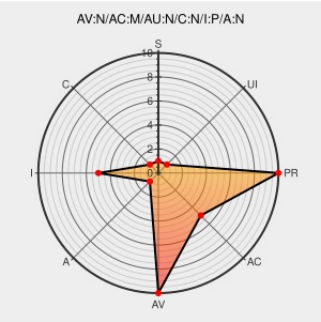
CVE-2006-0437

Published on: 02/06/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:05 PM UTC

CVE-2006-0437

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



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

Cross-site scripting (XSS) vulnerability in admin_smilies.php in phpBB 2.0.19 allows remote attackers to inject arbitrary web script or HTML via Javascript events such as "onmouseover" in the (1) smile_url or (2) smile_emotion parameters, which bypasses a check for "<" and ">" characters.

CVE-2006-0437 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
SecurityReason - phpBB 2.0.19 Cross Site Request Forgeries and XSS Admin	securityreason.com text/html	SREASON 406
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpbb-referer-header-http-xss(24497)
[Full-disclosure] phpBB 2.0.19 Cross Site Request Forgeries and XSS Admin	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060203 phpBB 2.0.19 Cross Site Request Forgeries and XSS Admin
phpBB "Referer" Header Session ID Disclosure - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18693

No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 22928
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-0445
SecurityReason - phpBB 2.0.19 Cross Site Request Forgeries and XSS Admin	Exploit securityreason.com text/html	SREASONRES 20060203 phpBB 2.0.19 Cross Site Request Forgeries and XSS Admin

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	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.11	All	All	All
Application	Phpbb Group	Phpbb	2.0.12	All	All	All
Application	Phpbb Group	Phpbb	2.0.13	All	All	All
Application	Phpbb Group	Phpbb	2.0.14	All	All	All
Application	Phpbb Group	Phpbb	2.0.15	All	All	All
Application	Phpbb Group	Phpbb	2.0.16	All	All	All
Application	Phpbb Group	Phpbb	2.0.17	All	All	All
Application	Phpbb Group	Phpbb	2.0.18	All	All	All
Application	Phpbb Group	Phpbb	2.0.19	All	All	All
Application	Phpbb Group	Phpbb	2.0.6c	All	All	All
Application	Phpbb Group	Phpbb	2.0.6d	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.7a	All	All	All
Application	Phpbb Group	Phpbb	2.0.8	All	All	All
Application	Phpbb Group	Phpbb	2.0.8a	All	All	All
Application	Phpbb Group	Phpbb	2.0.9	All	All	All
Application	Phpbb Group	Phpbb	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.11	All	All	All
Application	Phpbb Group	Phpbb	2.0.12	All	All	All
Application	Phpbb Group	Phpbb	2.0.13	All	All	All
Application	Phpbb Group	Phpbb	2.0.14	All	All	All

Application	Phpbb Group	Phpbb	2.0.15	All	All	All
Application	Phpbb Group	Phpbb	2.0.16	All	All	All
Application	Phpbb Group	Phpbb	2.0.17	All	All	All
Application	Phpbb Group	Phpbb	2.0.18	All	All	All
Application	Phpbb Group	Phpbb	2.0.19	All	All	All
Application	Phpbb Group	Phpbb	2.0.6c	All	All	All
Application	Phpbb Group	Phpbb	2.0.6d	All	All	All
Application	Phpbb Group	Phpbb	2.0.7	All	All	All
Application	Phpbb Group	Phpbb	2.0.7a	All	All	All
Application	Phpbb Group	Phpbb	2.0.8	All	All	All
Application	Phpbb Group	Phpbb	2.0.8a	All	All	All
Application	Phpbb Group	Phpbb	2.0.9	All	All	All

cpe:2.3:a:phpbb_group:phpbb:2.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.16:*:*:*:*:*:*:*:

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

cpe:2.3:a:phpbb_group:phpbb:2.0.18:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.19:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.6c:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.6d:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.7a:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.8a:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.16:*:*:*:*:*:*:*:

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

cpe:2.3:a:phpbb_group:phpbb:2.0.18:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.19:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.6c:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.6d:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.7a:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.8a:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→