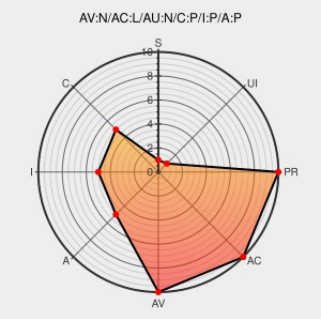
CVE-2004-1315

Published on: 11/12/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1315

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



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

viewtopic.php in phpBB 2.x before 2.0.11 improperly URL decodes the highlight parameter when extracting words and phrases to highlight, which allows remote attackers to execute arbitrary PHP code by double-encoding the highlight value so that special characters are inserted into the result, which is then processed by PHP exec, as exploited by the Santy.A worm.

CVE-2004-1315 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
phpBB.com :: View topic - howdark.com exploits - follow up	Vendor Advisory www.phpbb.com text/html	CONFIRM www.phpbb.com/phpBB/viewtopic.php?t=240513
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpbb-view-sql-injection(18052)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20041222 Re: phpBB Worm
Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-200411-32
'EXEC exploit in phpBB - fix' thread - MARC	marc.info	BUGTRAQ 20041118 EXEC exploit

	text/html	in phpBB - fix
US-CERT Technical Cyber Security Alert TA04-356A -- Exploitation of phpBB highlight parameter vulnerability	Patch Third Party Advisory US Government Resource www.us-cert.gov text/html	CERT TA04-356A
phpBB Viewtopic.PHP PHP Script Injection Vulnerability	cve.report (archive) text/html	BID 10701
'phpBB Code EXEC (v2.0.10)' - MARC	marc.info text/html	BUGTRAQ 20041112 phpBB Code EXEC (v2.0.10)
US-CERT Vulnerability Note VU#497400	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#497400
Secunia - Advisories - phpBB Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 13239
'phpBB Worm' - MARC	marc.info text/html	BUGTRAQ 20041220 phpBB Worm

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	All	All	All	All
Application	Phpbb Group	Phpbb	1.0.0	All	All	All
Application	Phpbb Group	Phpbb	1.0.1	All	All	All
Application	Phpbb Group	Phpbb	1.2.0	All	All	All
Application	Phpbb Group	Phpbb	1.2.1	All	All	All
Application	Phpbb Group	Phpbb	1.4.0	All	All	All
Application	Phpbb Group	Phpbb	1.4.1	All	All	All
Application	Phpbb Group	Phpbb	1.4.2	All	All	All
Application	Phpbb Group	Phpbb	1.4.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.0	All	All	All
Application	Phpbb Group	Phpbb	2.0.1	All	All	All
Application	Phpbb Group	Phpbb	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.2	All	All	All

Application	Phpbb Group	Phpbb	2.0.3	All	All	All
Application	Phpbb Group	Phpbb	2.0.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.5	All	All	All
Application	Phpbb Group	Phpbb	2.0.6	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_beta1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc2	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc3	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc4	All	All	All
Application	Phpbb Group	Phpbb	All	All	All	All
Application	Phpbb Group	Phpbb	1.0.0	All	All	All
Application	Phpbb Group	Phpbb	1.0.1	All	All	All
Application	Phpbb Group	Phpbb	1.2.0	All	All	All
Application	Phpbb Group	Phpbb	1.2.1	All	All	All
Application	Phpbb Group	Phpbb	1.4.0	All	All	All
Application	Phpbb Group	Phpbb	1.4.1	All	All	All
Application	Phpbb Group	Phpbb	1.4.2	All	All	All
Application	Phpbb Group	Phpbb	1.4.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.0	All	All	All
Application	Phpbb Group	Phpbb	2.0.1	All	All	All
Application	Phpbb Group	Phpbb	2.0.10	All	All	All
Application	Phpbb Group	Phpbb	2.0.2	All	All	All
Application	Phpbb Group	Phpbb	2.0.3	All	All	All
Application	Phpbb Group	Phpbb	2.0.4	All	All	All
Application	Phpbb Group	Phpbb	2.0.5	All	All	All
Application	Phpbb Group	Phpbb	2.0.6	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	2.0.7	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_beta1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc1	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc2	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc3	All	All	All
Application	Phpbb Group	Phpbb	2.0_rc4	All	All	All

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

cpe:2.3:a:phpbb_group:phpbb:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.1:*:*:*:*:*:*:*:

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

cpe:2.3:a:phpbb_group:phpbb:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.5:*:*:*:*:*:*:*:

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

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_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc3:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc4:*:*:*:*:*:*:*:

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

cpe:2.3:a:phpbb_group:phpbb:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.1:*:*:*:*:*:*:*:

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

cpe:2.3:a:phpbb_group:phpbb:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0.5:*:*:*:*:*:*:*:

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

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_beta1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc2:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc3:*:*:*:*:*:*:*:

cpe:2.3:a:phpbb_group:phpbb:2.0_rc4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→