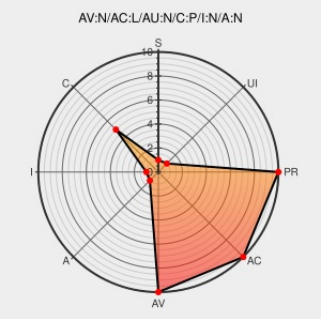
CVE-2005-0544

Published on: 02/24/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:26 PM UTC

CVE-2005-0544

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



Certain versions of Phpmyadmin from Phpmyadmin contain the following vulnerability:

phpMyAdmin 2.6.1 allows remote attackers to obtain the full path of the server via direct requests to (1) sqlvalidator.lib.php, (2) sqlparser.lib.php, (3) select_theme.lib.php, (4) select_lang.lib.php, (5) relation_cleanup.lib.php, (6) header_meta_style.inc.php, (7) get_foreign.lib.php, (8) display_tbl_links.lib.php, (9) display_export.lib.php, (10) db_table_exists.lib.php, (11) charset_conversion.lib.php, (12) ufpdf.php, (13) mysqli.dbi.lib.php, (14) setup.php, or (15) cookie.auth.lib.php, which reveals the path in a PHP error message.

CVE-2005-0544 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Gentoo Linux Documentation -- phpMyAdmin: Multiple vulnerabilities	Patch, Vendor Advisory, www.gentoo.org, text/html	GENTOO GLSA-200503-07
Secunia - Advisories - phpMyAdmin Local File Inclusion and Cross-Site Scripting	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 14382
SourceForge.net: Detail: 1149383 - (in 2.6.1-pl1)	Vendor Advisory	CONFIRM sourceforge.net/tracker/index.php?

SourceForge.net: Detail: 1149383 - (fi 2.6.1-pl1)
Possible XSS Attacks

Vendor Advisory
sourceforge.net
text/html

CONFIRM sourceforge.net/tracker/index.php?func=detail&aid=1149383&group_id=23067&atid=377408

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpmyadmin	Phpmyadmin	2.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1	All	All	All

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→