



CVE-2005-3300

Published on: 10/23/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

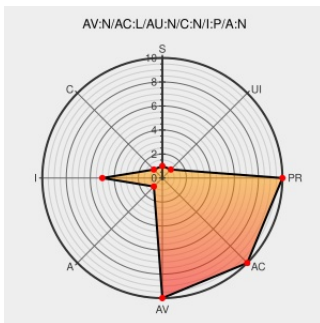
CVE-2005-3300

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Phpmyadmin](#) from [Phpmyadmin](#) contain the following vulnerability:

The register_globals emulation layer in grab_globals.php for phpMyAdmin before 2.6.4-pl3 does not perform safety checks on values in the _FILES array for uploaded files, which allows remote attackers to include arbitrary files by using direct requests to library scripts that do not use grab_globals.php, then modifying certain configuration values for the theme.

CVE-2005-3300 has been assigned by [M](#) 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
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Secunia - Advisories - SUSE update for phpmyadmin	web.archive.org text/html	X SECUNIA 17607
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpmyadmin-multiple-scripts-file-include(22835)
phpMyAdmin > Security MySQL Database Administration Tool www.phpmyadmin.net	Patch Vendor Advisory www.phpmyadmin.net text/html	CONFIRM www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-5
SecurityTracker.com Archives - phpMyAdmin 'grab_globals.php' Lets Remote Users Include and Execute Local Files	securitytracker.com text/html	SECTrack 1015091

No Description Provided	archives.neohapsis.com	FULLDISC 20051022 Advisory 16/2005: phpMyAdmin Local File Inclusion Vulnerability
	Inactive Link Not Archived	
phpMyAdmin Theme Variable Local File Inclusion Vulnerability	cve.report (archive) text/html	BID 15169
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:066
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	SECUNIA 17559
Gentoo Linux Documentation -- phpMyAdmin: Local file inclusion and XSS vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200510-21
Hardened-PHP Project - PHP Security - Advisory 16/2005	Patch Vendor Advisory www.hardened-php.net text/html	MISC www.hardened-php.net/advisory_162005.73.html
Secunia - Advisories - Debian update for phpmyadmin	web.archive.org text/html	SECUNIA 17337
'Advisory 16/2005: phpMyAdmin Local File Inclusion Vulnerability' - MARC	marc.info text/html	BUGTRAQ 20051022 Advisory 16/2005: phpMyAdmin Local File Inclusion Vulnerability
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:028
Debian -- Security Information -- DSA-880-1 phpmyadmin	www.debian.org Deprecated Link text/html	DEBIAN DSA-880
Secunia - Advisories - phpMyAdmin Local File Inclusion and Cross-Site Scripting	web.archive.org text/html	SECUNIA 17289

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	Phpmyadmin	Phpmyadmin	2.6.4_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.4_pl3	All	All	All
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.4_pl3:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.4_pl3:*****:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)