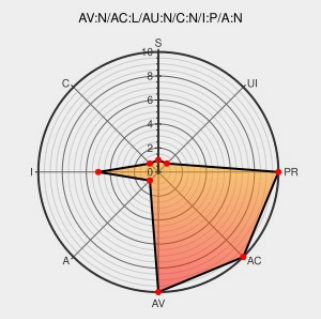
CVE-2005-3621

Published on: 11/16/2005 12:00:00 AM UTC

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

CVE-2005-3621

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



Certain versions of Phpmyadmin from Phpmyadmin contain the following vulnerability:

CRLF injection vulnerability in phpMyAdmin before 2.6.4-pl4 allows remote attackers to conduct HTTP response splitting attacks via unspecified scripts.

CVE-2005-3621 has been assigned by security@debian.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
SecurityTracker.com Archives - phpMyAdmin 'libraries/header_http.inc.php' Lets Remote Users Conduct HTTP Response Splitting Attacks	securitytracker.com, text/html	SECTRACK 1015213
Debian -- Security Information -- DSA-1207-2 phpmyadmin	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-1207
Debian update for phpmyadmin - Advisories - Secunia	web.archive.org, text/html	SECUNIA 22781
Secunia - Advisories - phpMyAdmin HTTP Response Splitting and Cross-Site Scripting	web.archive.org, text/html	SECUNIA 17578
Security Announcement	web.archive.org, text/html, Inactive Link, Not Archived	SUSE SUSE-SR:2005:028

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-2005-6

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	2.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.2_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.3_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.4_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.2_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.3_pl1	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.6.4_pl3	All	All	All

- cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.0:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.7_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc2:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.2_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.3_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.4_pl3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.0:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.7_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc2:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl3:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.2_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.3_pl1:*:*:*:*:*:*:*:
- cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.4_pl3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→