



CVE-2015-2206

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-2206
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-09 17:59:00 UTC
Updated	2016-12-28 02:59:00 UTC
Description	libraries/select_lang.lib.php in phpMyAdmin 4.0.x before 4.0.10.9, 4.2.x before 4.2.13.2, and 4.3.x before 4.3.11.1 includes

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc3	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.6	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.0.10.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.7.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.11	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc3	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.4.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.11	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.2.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.7.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.9	All	All	All

References						
Reference	Source	Link	Tags			
openSUSE-SU-2015:1191-1: moderate: Security update for phpMyAdmin	SUSE	lists.opensuse.org				
[SECURITY] Fedora 20 Update: phpMyAdmin-4.3.11.1-1.fc20	FEDORA	lists.fedoraproject.org	Third Party Adv			
[security] Risk of BREACH attack · phpmyadmin/phpmyadmin@b2f1e89 · GitHub	CONFIRM	github.com				
phpMyAdmin Bug May Disclose CSRF Token to Remote Users - SecurityTracker	SECTrack	www.securitytracker.com	Third Party Adv			
Debian -- Security Information -- DSA-3382-1 phpmyadmin	DEBIAN	www.debian.org				
phpMyAdmin - Security - PMASA-2015-1	CONFIRM	www.phpmyadmin.net	Vendor Advisor			

phpMyAdmin CVE-2015-2206 Information Disclosure Vulnerability	BID	www.securityfocus.com	
Support / Security / Advisories // MDVSA-2015:186 Mandriva	MANDRIVA	www.mandriva.com	Broken Link
[SECURITY] Fedora 22 Update: phpMyAdmin-4.3.11.1-1.fc22	FEDORA	lists.fedoraproject.org	Third Party Adv
[SECURITY] Fedora 21 Update: phpMyAdmin-4.3.11.1-1.fc21	FEDORA	lists.fedoraproject.org	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report