



CVE-2015-3903

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

Summary

CVE	CVE-2015-3903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-26 15:59:00 UTC
Updated	2018-10-09 19:56:00 UTC
Description	libraries/Config.class.php in phpMyAdmin 4.0.x before 4.0.10.10, 4.2.x before 4.2.13.3, 4.3.x before 4.3.13.1, and 4.4.x before 4.4.12.1

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	4.0.10.2	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	4.0.10.9	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	4.2.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.2	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	4.2.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.7.1	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	4.3.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.13	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	4.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.4.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6	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	4.0.10.2	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	4.0.10.9	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	4.2.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.2.13.2	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	4.0.5	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.2.5	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	4.2.9.1	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	4.3.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.3.13	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	4.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.6	All	All	All

References

Reference

openSUSE-SU-2015:1191-1: moderate: Security update for phpMyAdmin

phpMyAdmin Github API Call Certificate Validation Bypass Lets Remote Users Obtain and Modify Potentially Sensitive Data - SecurityTracker

phpMyAdmin 4.4.6 Man-In-the-Middle to API Github - CXSecurity.com

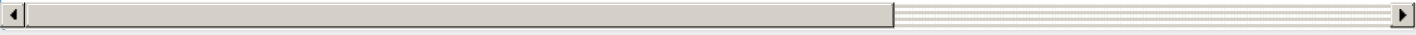
phpMyAdmin CVE-2015-3903 Man in the Middle Security Bypass Vulnerability

Debian -- Security Information -- DSA-3382-1 phpmyadmin

phpMyAdmin - Security - PMASA-2015-3

phpMyAdmin 4.4.6 Man-In-The-Middle ≈ Packet Storm

bug #4900 [security] Vulnerability allowing man-in-the-middle attack · phpmyadmin/phpmyadmin@5ebc4da · GitHub

SecurityFocus
CVE Program record
NVD vulnerability detail

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](#)