



CVE-2014-8961

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

Summary

CVE	CVE-2014-8961
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-30 11:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Directory traversal vulnerability in libraries/error_report.lib.php in the error-reporting feature in phpMyAdmin 4.1.x before 4.1

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.4	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.1.14.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.9	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	4.2.2	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	4.2.7.1	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	4.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.4	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.1.14.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.14.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.1.9	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	4.2.2	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	4.2.7.1	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

References						
Reference					Source	Link
openSUSE-SU-2014:1561-1: moderate: Security update for phpMyAdmin					SUSE	lists.opensuse.org
Gentoo Security					GENTOO	security.gentoo.org
Support / Security / Advisories / / MDVSA-2014:228 Mandriva					MANDRIVA	www.mandriva.com
phpMyAdmin Error Reporting Feature Information Disclosure Vulnerability					BID	www.securityfocus.com
phpMyAdmin - Security - PMASA-2014-16					CONFIRM	www.phpmyadmin.org
bug #4595 [security] Path traversal can lead to leakage of line count · phpmyadmin/phpmyadmin@b99b6b6 · GitHub					CONFIRM	github.com
CVE Program record					CVE.ORG	www.cve.org
NVD vulnerability detail					NVD	nvd.nist.gov

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](#)