



CVE-2016-2043

Published on: 02/19/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2043

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-site scripting (XSS) vulnerability in the goToFinish1NF function in js/normalization.js in phpMyAdmin 4.4.x before 4.4.15.3 and 4.5.x before 4.5.4 allows remote authenticated users to inject arbitrary web script or HTML via a table name to the normalization page.

CVE-2016-2043 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
openSUSE-SU-2016:0357-1: moderate: Security update for phpMyAdmin	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0357
[SECURITY] Fedora 23 Update:	Third Party Advisory	FEDORA FEDORA-2016-e55278763e

phpMyAdmin-4.5.4.1-1.fc23	lists.fedoraproject.org text/html	
openSUSE-SU-2016:0378-1: moderate: Security update to phpMyAdmin 4.4.15.	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0378
[SECURITY] Fedora 22 Update: phpMyAdmin-4.5.4-1.fc22	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-e1fe01e96e
Fix XSS in normalization.php - phpmyadmin/phpmyadmin@019c4f2 · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/019c4f25d500ec5db9ba3b84cc9
phpMyAdmin - Security - PMASA- 2016-7	Patch Vendor Advisory www.phpmyadmin.net text/html	 CONFIRM www.phpmyadmin.net/home_page/security/PMASA-2016-7.php

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
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	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	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.1	All	All	All
Application	Phnmvadmin	Phnmvadmin	4.4.1.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	Version	OS	OS	OS
Application	Phpmyadmin	Phpmyadmin	4.4.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.14.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.2	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	4.4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.3	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	4.4.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.12	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.13.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.14.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.4.15.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.2	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	4.4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.3	All	All	All
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.1:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.1.1:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.10:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.11:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.12:*:*:*:*:*:						

cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.13:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.13.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.14.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.6.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.8:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.9:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.10:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.11:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.12:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.13:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.13.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.14.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.6.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.8:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.9:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.3:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© 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](#).

