

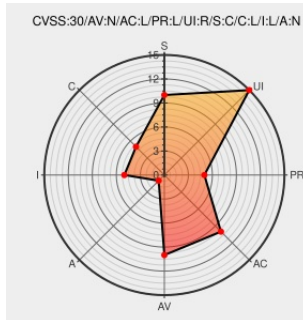


CVE-2016-2561

Published on: 03/01/2016 12:00:00 AM UTC

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

CVE-2016-2561

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.5 and 4.5.x before 4.5.5.1 allow remote authenticated users to inject arbitrary web script or HTML via (1) normalization.php or (2) js/normalization.js in the database normalization page, (3) templates/database/structure/sortable_header.phtml in the database structure page, or (4) the pos parameter to db_central_columns.php in the central columns page.

CVE-2016-2561 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
Debian Security Information	CVE-2016-2561	DEBIAN DSA-3607

Debian -- Security information -- DSA-3627-1 phpmyadmin	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3627
[SECURITY] Fedora 23 Update: phpMyAdmin-4.5.5.1-1.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-65da02b95c
openSUSE-SU-2016:0666-1: moderate: Security update for phpMyAdmin	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0666
[SECURITY] Fedora 22 Update: phpMyAdmin-4.5.5.1-1.fc22	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-02ee5b4002
Fix XSS in normalization.js · phpmyadmin/phpmyadmin@f33a42f · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/f33a42f1da9db943a67bda7d29
openSUSE-SU-2016:0663-1: moderate: Security update for phpMyAdmin	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0663
Fix XSS in normalization.js · phpmyadmin/phpmyadmin@bcd4ce8 · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/bcd4ce8cba1272fca52f2331c0f
Fix XSS in database structure page · phpmyadmin/phpmyadmin@983faa9 · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/983faa94f161df3623ecd371d3f
phpMyAdmin - Security - PMASA- 2016-12	Patch Vendor Advisory www.phpmyadmin.net text/html	 CONFIRM www.phpmyadmin.net/security/PMASA-2016-12/
Fix XSS in normalization · phpmyadmin/phpmyadmin@746240b · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/746240bd13b62b5956fc34389c
Escape selectors · phpmyadmin/phpmyadmin@37c34d0 · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/37c34d089aa19f30d11203bb0c
Fix XSS in Central columns page · phpmyadmin/phpmyadmin@cc55f44 · GitHub	Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/cc55f44a4a90147a007dee1aef

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
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	4.4.10	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	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	4.4.15.4	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	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	beta2	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	rc1	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	4.5.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.5	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	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	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	4.4.15.4	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	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	beta2	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.0	rc1	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	4.5.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.4.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.5.5	All	All	All

cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.0:****:*:
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:****:*:
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:4.4.15.4:****:*:
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:beta1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:beta2:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:rc1:****:*:

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:4.5.3.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.4.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.0:*****:
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:*****:
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:4.4.15.4:*****:
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:beta1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:beta2:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.0:rc1:~::~::~::~:
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:4.5.3.1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.4:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.4.1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.5.5:~::~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)