

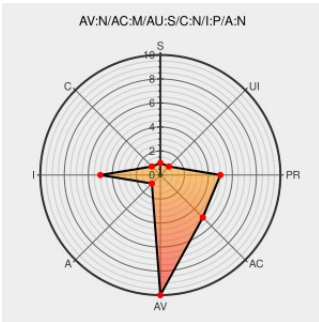


CVE-2014-5273

Published on: 08/21/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

CVE-2014-5273

[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 4.0.x before 4.0.10.2, 4.1.x before 4.1.14.3, and 4.2.x before 4.2.7.1 allow remote authenticated users to inject arbitrary web script or HTML via the (1) browse table page, related to js/sql.js; (2) ENUM editor page, related to js/functions.js; (3) monitor page, related to js/server_status_monitor.js; (4) query charts page, related to js/tbl_chart.js; or (5) table relations page, related to libraries/tbl_relation.lib.php.

CVE-2014-5273 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

SINGLE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description	Tags	Link
bug #4502 [security] Self-XSS in enum value editor · phpmyadmin/phpmyadmin@2c45d7c · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/phpmyadmin/phpmyadmin/commit/2c45d7caa614afd71dbe3d0f72
openSUSE-SU-2014:1069-1: moderate: update for phpMyAdmin	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:1069
bug #4501 [security] XSS in table browse page · phpmyadmin/phpmyadmin@647c9d1 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/phpmyadmin/phpmyadmin/commit/647c9d12e33a6b64e1c3ff7487

bug #4503 [security] Self-XSSes in monitor · phpmyadmin/phpmyadmin@cd9f302 · GitHub	Exploit Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/cd9f302bf7f91a160fe7080f9a61
About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 60397
bug #4517 [security] XSS in relation view · phpmyadmin/phpmyadmin@3ffc967 · GitHub	Exploit Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/3ffc967fb60cf2910cc2f571017e
bug #4504 [security] Self-XSS in query charts · phpmyadmin/phpmyadmin@90ddeec · GitHub	Exploit Patch github.com text/html	 CONFIRM github.com/phpmyadmin/phpmyadmin/commit/90ddeecf60fc029608b972e490
phpMyAdmin - Security - PMASA-2014-8	Vendor Advisory www.phpmyadmin.net text/html	 CONFIRM www.phpmyadmin.net/home_page/security/PMASA-2014-8.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
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	4.0.2	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	4.1.0	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	4.1.2	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	4.2.2	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	4.0.0	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	4.0.2	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	4.1.0	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	4.1.2	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	4.2.2	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
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc2:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc3:*:*:*:*:						

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.1:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.1:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.2:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.3:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4.1:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4.2:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.5:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.6:::*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.7:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.8:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.9:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.1:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.10:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.11:::*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.12:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14.*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14.1:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14.2:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.5:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.7:*:*:*:*:*:*:*:
```

cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.8:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.9:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.4.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.8:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.9:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.10:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.11:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.12:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.13:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.14.2:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.2:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.3:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.4:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.5:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.6:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.7:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.8:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.1.9:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.2:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.3:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.4:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.5:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.6:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.2.7:****:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)