



CVE-2016-6615

Published on: 12/10/2016 12:00:00 AM UTC

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

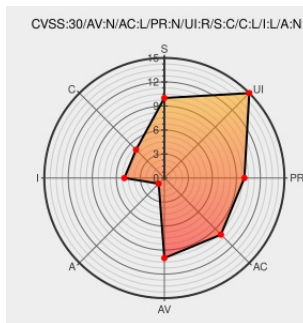
CVE-2016-6615

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

XSS issues were discovered in phpMyAdmin. This affects navigation pane and database/table hiding feature (a specially-crafted database name can be used to trigger an XSS attack); the "Tracking" feature (a specially-crafted query can be used to trigger an XSS attack); and GIS visualization feature. All 4.6.x versions (prior to 4.6.4) and 4.4.x versions (prior to 4.4.15.8) are affected.

CVE-2016-6615 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 1415-1] phpmyadmin security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20180706 [SECURITY] [DLA 1415-1] phpmyadmin security update

phpMyAdmin: Multiple vulnerabilities (GLSA 201701-32) — Gentoo security

[security.gentoo.org](https://security.gentoo.org/text/html)
text/html

 GENTOO GLSA-201701-32

phpMyAdmin - Security - PMASA-2016-38

[Patch](#)
[Vendor Advisory](#)
www.phpmyadmin.net
text/html

 CONFIRM www.phpmyadmin.net/security/PMASA-2016-38

phpMyAdmin CVE-2016-6615 Multiple Cross Site Scripting Vulnerabilities

[cve.report \(archive\)](#)
text/html

 BID 95041

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.

Related QID Numbers

[710467](#) Gentoo Linux Hypertext Preprocessor (PHP) MyAdmin Multiple Vulnerabilities (GLSA 201701-32)

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	4.4.14.1	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	4.4.15.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.7	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	4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	alpha1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.3	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	4.4.10	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	4.4.15.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.4.15.7	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	4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	alpha1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.6.3	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:4.4.14.1:*:*:*:*:*:						
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:4.4.15.5:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.6:*:*:*:*:*:						
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.7:*:*:*:*:*:						
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:4.6.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:alpha1:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.2:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.3:*:*:*:*:*:*:*:
```

```
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:4.4.14.1:*.~*~*~*~*~*
```

```
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:4.4.15.5:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.6:*:*:*:*:*:
```

cpe:2.3:a:phpmyadmin:phpmyadmin:4.4.15.7:~::~::~::~:
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:4.6.0:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:alpha1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:rc1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.0:rc2:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.1:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.2:~::~::~::~:
cpe:2.3:a:phpmyadmin:phpmyadmin:4.6.3:~::~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)