



CVE-2015-8669

Published on: 12/26/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-8669

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

libraries/config/messages.inc.php in phpMyAdmin 4.0.x before 4.0.10.12, 4.4.x before 4.4.15.2, and 4.5.x before 4.5.3.1 allows remote attackers to obtain sensitive information via a crafted request, which reveals the full path in an error message.

CVE-2015-8669 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
[Security] Path disclosure, see PMASA-2015-6 · phpmyadmin/phpmyadmin@c4d6493 · GitHub	github.com text/html	CONFIRM github.com/phpmyadmin/phpmyadmin/commit/c4d649325b25139d7c097e5

openSUSE-SU-2016:0067-1:
moderate: Security update for
phpMyAdmin

lists.opensuse.org
text/html

 SUSE openSUSE-SU-2016:0067

phpMyAdmin - Security - PMASA-
2015-6

Vendor Advisory
www.phpmyadmin.net
text/html

 CONFIRM www.phpmyadmin.net/security/PMASA-2015-6/

phpMyAdmin Include File Access
Flaw Lets Remote Users View File
Path Information - SecurityTracker

www.securitytracker.com  [SECTrack 1034806](#)
text/html

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	4.0.1	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	4.0.10.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.9	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	4.4.0	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	4.4.2	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	4.0.0	All	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	4.0.10.10	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All

Application	Phpmyadmin	Phpmyadmin	4.0.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.10.9	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	4.4.0	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	4.4.2	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	Phpmysql	Phpmysql	4.4.8	All	All	All
Application	Phpmysql	Phpmysql	4.4.9	All	All	All
Application	Phpmysql	Phpmysql	4.5.0	All	All	All
Application	Phpmysql	Phpmysql	4.5.0.1	All	All	All
Application	Phpmysql	Phpmysql	4.5.0.2	All	All	All
Application	Phpmysql	Phpmysql	4.5.1	All	All	All
Application	Phpmysql	Phpmysql	4.5.2	All	All	All
Application	Phpmysql	Phpmysql	4.5.3	All	All	All

cpe:2.3:a:phpmysql:phpmysql:4.0.0:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.1:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.1:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.10:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.11:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.2:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.3:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.4:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.5:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.6:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.7:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.8:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.10.9:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.2:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.3:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.4:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.4.1:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.4.2:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.5:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql:4.0.6:*:*:*:*:*:

cpe:2.3:a:phpmysql:phpmysql: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:4.4.0:*:*:*:*:*:*:
```

```
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:4.4.2:*:*:*:*:*:*:*
```

```
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:4.0.0:*:*:*:*:*:*:
```

```
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:4.0.10.10:*:*:*:*:*.*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.11:*:*:*:*:*.*.*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.2:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.3:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.4:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.5:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.6:::*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.7:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.8:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.10.9:*:*:*:*:*:*
```

```
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:4.4.0:*:*:*:*:*:*:
```

```
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:4.4.2:*:*:*:*:*:
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](#).

CVE.report and Source URL Uptime Status status.cve.report