

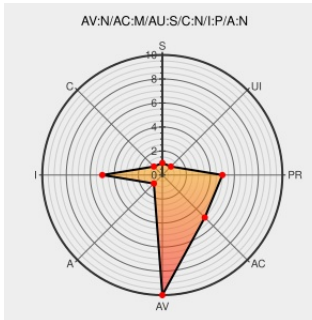


CVE-2012-4345

Published on: 08/21/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2012-4345

[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 the Database Structure page in phpMyAdmin 3.4.x before 3.4.11.1 and 3.5.x before 3.5.2.2 allow remote authenticated users to inject arbitrary web script or HTML via (1) a crafted table name during table creation, or a (2) Empty link or (3) Drop link for a crafted table name.

CVE-2012-4345 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

No Description Provided

hermes.opensuse.org

[SUSE openSUSE-SU-2012:1062](#)

Inactive Link **Not Archived**

Support / Security / Advisories // MDVSA-2012:136 | Mandriva

www.mandriva.com

[text/html](#)

[MANDRIVA MDVSA-2012:136](#)

phpMyAdmin - Security - PMASA-2012-4

[Patch](#)

[Vendor Advisory](#)

www.phpmyadmin.net

[text/html](#)

[CONFIRM](#)

www.phpmyadmin.net/home_page/security/PMASA-2012-4.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,

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	3.4.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.7.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.7.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.8.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.10.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.11	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	3.4.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.6.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.7.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.7.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.8.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.1	All	All	All
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.0.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.1.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.1:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.2:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.11:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.2.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.1:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.2:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.4.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.5.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.6.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.7.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.7.1:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.8.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.9.0:*****:						
cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.0.0:*****:						

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.1.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.1:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.0.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.1.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.1:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.10.2:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.11:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.2.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.1:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.2:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.4.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.5.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.6.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.7.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.7.1:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.8.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.9.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.0.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.1.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.0:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

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](#)