



CVE-2007-1395

Published on: 03/10/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:36 PM UTC

CVE-2007-1395

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Incomplete blacklist vulnerability in index.php in phpMyAdmin 2.8.0 through 2.9.2 allows remote attackers to conduct cross-site scripting (XSS) attacks by injecting arbitrary JavaScript or HTML in a (1) db or (2) table parameter value followed by an uppercase `</SCRIPT>` end tag, which bypasses the protection against lowercase `</script>`.

CVE-2007-1395 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20070307 xss in phpmyadmin >=2.8.0 and < 2.10.0](#)

No Description Provided

osvdb.org

[OSVDB 35048](#)

Inactive Link Not Archived

Debian update for phpmyadmin - Advisories - Secunia

web.archive.org
text/html

[SECUNIA 26733](#)

Security Advisories | Mandriva Linux

www.mandriva.com
text/html

[MANDRIVA MDKSA-2007:199](#)

SecurityReason - xss in phpmyadmin >=2.8.0 and < 2.10.0

securityreason.com
text/html

[SREASON 2402](#)

Debian -- Security Information -- DSA-1370-1
phpmyadmin

web.archive.org

[text/html](#)

Inactive Link Not Archived

 [DEBIAN DSA-1370](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

[text/html](#)

 [XF phpmyadmin-dbtable-xss\(32858\)](#)

No Description Provided

[Exploit](#)

[Vendor Advisory](#)

www.virtuax.be

 [MISC www.virtuax.be/advisories/Advisory2-24012007.txt](https://www.virtuax.be/advisories/Advisory2-24012007.txt)

Inactive Link Not Archived

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	2.8.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.1_dev	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_beta1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_dev	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1_rc2	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.9.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.1_dev	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.8.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_beta1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_dev	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.0_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.1_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.9.2	All	All	All
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.1:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.2:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.3:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.1:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.1_dev:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.2:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.3:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.4:*:*:*:*:*.*						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9:*:*:*:*:*.*						

cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_beta1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_dev:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1_rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.0.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.1_dev:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.8.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_beta1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_dev:*****:

cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.0_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.1_rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.9.2:*****:

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](#)