



CVE-2005-0992

Published on: 04/07/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:26 PM UTC

CVE-2005-0992

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Cross-site scripting (XSS) vulnerability in index.php in phpMyAdmin before 2.6.2-rc1 allows remote attackers to inject arbitrary web script or HTML via the convcharset parameter.

CVE-2005-0992 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

PHPMYAdmin Convcharset Cross-Site Scripting Vulnerability

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

[🌐](#) [BID 12982](#)

phpMyAdmin Cross-site Scripting Vulnerability

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[🌐](#) [MISC](#)
www.arrelnet.com/advisories/adv20050403.html

'phpMyAdmin Cross-site Scripting Vulnerability' - MARC

[marc.info](#)
[text/html](#)

[🌐](#) [BUGTRAQ 20050404 phpMyAdmin Cross-site Scripting Vulnerability](#)

Gentoo Linux Documentation -- phpMyAdmin: Cross-site scripting vulnerability

[Patch](#)
[Vendor Advisory](#)
[www.gentoo.org](#)
[text/html](#)

[🌐](#) [GENTOO GLSA-200504-08](#)

Secunia - Advisories - phpMyAdmin "convcharset" Cross-Site Scripting Vulnerability	Vendor Advisory web.archive.org text/html	 SECUNIA 14799
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF phpmyadmin-convcharset-xss(19940)
phpMyAdmin > Security MySQL Database Administration Tool www.phpmyadmin.net	Vendor Advisory www.phpmyadmin.net text/html	 CONFIRM www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-3

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	2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_pre1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_pre2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.3.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.0.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2.6	All	All	All

Application	Phpmyadmin	Phpmyadmin	2.2_pre1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_pre2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.2_rc3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.5_rc2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.6_rc1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.5.7_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl2	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.0_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl1	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_pl3	All	All	All
Application	Phpmyadmin	Phpmyadmin	2.6.1_rc1	All	All	All
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.1:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.2:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.3:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.4:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.5:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.6:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.7:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.8:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.9:*:*:*:*:*.*.*.						
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1:*:*:*:*:*.*.*.						

cpe:2.3:a:phpmyadmin:phpmyadmin:2.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_pre1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_pre2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.3.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.3.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.4.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*****:

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl1:::*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl2:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl3:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl1:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl3:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_rc1.*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.2:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.3:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.4:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.0.5:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.2:*:*:*:*:*:*:*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_pre1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_pre2:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc1:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc2:*:*:*:*:*:*:
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.2_rc3:*:*:*:*:*.*
```

```
cpe:2.3:a:phpmyadmin:phpmyadmin:2.3.1:*:*:*:*:*:*:
```

cpe:2.3:a:phpmyadmin:phpmyadmin:2.3.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.4.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.4:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_pl1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.5_rc2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.6_rc1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.5.7_pl1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl2:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.0_pl3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_pl3:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:2.6.1_rc1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

