



CVE-2011-2506

Published on: 07/14/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:21 PM UTC

CVE-2011-2506

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

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

setup/lib/ConfigGenerator.class.php in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 does not properly restrict the presence of comment closing delimiters, which allows remote attackers to conduct static code injection attacks by leveraging the ability to modify the SESSION superglobal array.

CVE-2011-2506 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - Re:
CVE Request:
phpMyAdmin 3.4
Multiple Vulnerabilities

www.openwall.com
[text/html](#)

[MLIST \[oss-security\] 20110628 Re: CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities](#)

phpMyAdmin Multiple
Vulnerabilities -
Secunia.com

[Vendor Advisory](#)
web.archive.org
[text/html](#)

[SECUNIA 45139](#)

Haxxor Security:
phpMyAdmin 3.x
Multiple Remote Code
Executions

[Exploit](#)
ha.xxor.se
[text/html](#)

MISC ha.xxor.se/2011/07/phpmyadmin-3x-multiple-remote-code.html

www.xxor.se

[MISC](#)

	text/plain Inactive Link Not Archived	www.xxor.se/advisories/phpMyAdmin_3.x_Multiple_Remote_Code_Executions.txt
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 73612
phpMyAdmin / None tools	Patch phpmyadmin.git.sourceforge.net text/html	 CONFIRM phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/phpmyadmin;a=commit;h=0fbdaf5fd7a771d0885c6b7385d934fc90
phpMyAdmin 3.x Swekey Remote Code Injection Exploit	Exploit www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 17514
phpMyAdmin - Security - PMASA-2011-6	Patch Vendor Advisory www.phpmyadmin.net text/html	 CONFIRM www.phpmyadmin.net/home_page/security/PMASA-2011-6.php
[SECURITY] Fedora 14 Update: phpMyAdmin-3.4.3.1-1.fc14	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-9144
Fedora update for phpMyAdmin - Secunia.com	web.archive.org text/html	 SECUNIA 45292
Debian update for phpmyadmin - Secunia.com	web.archive.org text/html	 SECUNIA 45315
Debian -- Security Information -- DSA-2286-1 phpmyadmin	www.debian.org Depreciated Link text/html	 DEBIAN DSA-2286
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20110707 phpMyAdmin 3.x Multiple Remote Code Executions
oss-security - Re: CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities	www.openwall.com text/html	 MLIST [oss-security] 20110629 Re: CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities
Security Advisories Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDVSA-2011:124
oss-security - Re: [Phpmyadmin-security] CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities	www.openwall.com text/html	 MLIST [oss-security] 20110628 Re: [Phpmyadmin-security] CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities
TYPO3 - the Enterprise Open Source CMS: TYPO3 Security Bulletin TYPO3-SA-2011-008	typo3.org text/html	 CONFIRM typo3.org/teams/security/security-bulletins/typo3-sa-2011-008/
oss-security - CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities	www.openwall.com text/html	 MLIST [oss-security] 20110628 CVE Request: phpMyAdmin 3.4 Multiple Vulnerabilities

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	3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	alpha	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	beta	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.2	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	rc1	All	All
Application	Phomvadmin	Phomvadmin	3.2.1	All	All	All

Application	Phpmyadmin	Phpmyadmin	Version	Platform	Architecture	License
Application	Phpmyadmin	Phpmyadmin	3.2.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.10.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.2	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	3.4.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.4.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	alpha	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	beta	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.0.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.2	All	All	All

Application	Phpmyadmin	Phpmyadmin	3.1.2	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.3.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.4	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.1.5	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	beta1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.0	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.1	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.2.2	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.10.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.10.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.4.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.5.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.5.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.8	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.8.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.3.9.2	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	3.4.2.0	All	All	All

Application	Phpmyadmin	Phpmyadmin	3.4.3.0	All	All	All
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:alpha:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:beta:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1.1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:beta1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3.1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3.2:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.4:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.4:rc2:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.5:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.5:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:beta1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.1:rc1:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.2:*:*:*:*:*:
						cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.2:rc1:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.0.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.1.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.10.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.10.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.2.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.3.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.4.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.5.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.5.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.6:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.7:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.8:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.8.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.2:****:*:*:
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:3.4.2.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:alpha:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:beta:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.0:rc1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1:rc1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.0.1.1:****:*:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:****:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:beta1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3.1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3.2:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.4:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.4:rc2:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.5:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.5:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:beta1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.0:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.1:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.2:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.2.2:rc1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.0.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.1.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.10.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.10.1:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.2.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.3.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.4.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.5.0:****:*:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.5.1:****:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.6:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.7:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.8:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.8.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.1:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.3.9.2:*****:
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:3.4.2.0:*****:
cpe:2.3:a:phpmyadmin:phpmyadmin:3.4.3.0:*****:

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](#)