



CVE-2004-0129

Published on: 03/03/2004 05:00:00 AM UTC

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

CVE-2004-0129

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Directory traversal vulnerability in export.php in phpMyAdmin 2.5.5 and earlier allows remote attackers to read arbitrary files via .. (dot dot) sequences in the what parameter.

CVE-2004-0129 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF phpmyadmin-dotdot-directory-traversal\(15021\)](#)

'Arbitrary File Disclosure Vulnerability in phpMyAdmin 2.5.5-pl1 and prior' - MARC

[marc.info](https://marc.info/text/html)
text/html

[BUGTRAQ 20040203 Arbitrary File Disclosure Vulnerability in phpMyAdmin 2.5.5-pl1 and prior](#)

No Description Provided

www.osvdb.org

[OSVDB 3800](#)

Inactive Link Not Archived

Page not found - SourceForge.net

[sourceforge.net](https://sourceforge.net/text/html)
text/html

[CONFIRM sourceforge.net/forum/forum.php?forum_id=350228](#)

Inactive Link Not Archived

Gentoo Linux Documentation -- phpMyAdmin < 2.5.6-rc1: possible attack against export.php

[Vendor Advisory](#)
security.gentoo.org

[GENTOO GLSA-200402-05](#)

[text/html](#)

phpMyAdmin Export.PHP File Disclosure Vulnerability

[Exploit](#) BID 9564[Patch](#)[Vendor Advisory](#)[cve.report \(archive\)](#)[text/html](#)phpMyAdmin > Downloads | MySQL Database
Administration Tool | www.phpmyadmin.net[www.phpmyadmin.net](#)[text/html](#) CONFIRM
[www.phpmyadmin.net/home_page/relnotes.php?
rel=0](http://www.phpmyadmin.net/home_page/relnotes.php?rel=0)Secunia - Advisories - phpMyAdmin "export.php"
Directory Traversal Vulnerability[web.archive.org](#)[text/html](#) SECUNIA 10769

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	2.2.2	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_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	2.5.4	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	2.0	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	2.2.2	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_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	2.5.4	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
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:2.2.2:*:*:*:*:*:						
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_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:2.5.4:*:*:*:*:*:						
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:2.0:*:*:*:*:*:*:
```

```
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:2.2.2:*:*:*:*:*:*:*
```

```
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_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:2.5.4:*:*:*:*:*:
```

```
cpe:2.3:a:phomvadmin:phomvadmin: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:****:****:	
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](#)