

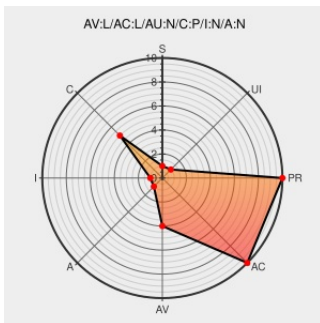


CVE-2006-1608

Published on: 04/10/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1608

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

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

The copy function in file.c in PHP 4.4.2 and 5.1.2 allows local users to bypass safe mode and read arbitrary files via a source argument containing a compress.zlib:// URI.

CVE-2006-1608 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060723 Re: new shell bypass safe mode](#)

Ubuntu update for PHP - Advisories - Secunia

web.archive.org
text/html

[SECUNIA 21125](#)

PHP copy() Function Safe Mode Checking Error Lets Users Bypass Safe Mode File Access Restrictions - SecurityTracker

securitytracker.com
text/html

[SECTrack 1015882](#)

usn/usn-320-1 - Ubuntu: Linux for human beings

www.ubuntu.com
text/html

[UBUNTU USN-320-1](#)

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060409 copy\(\) Safe Mode Bypass PHP 4.4.2 and 5.1.2](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com

[VUPEN ADV-2006-1290](#)

	text/html	
PHP Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities	cve.report (archive) text/html	BID 17439
SecurityReason - copy() Safe Mode Bypass PHP 4.4.2 and 5.1.2	Exploit Patch securityreason.com text/html	SREASONRES 20060408 copy() Safe Mode Bypass PHP 4.4.2 and 5.1.2
SecurityReason - copy() Safe Mode Bypass PHP 4.4.2 and 5.1.2	securityreason.com text/html	SREASON 678
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24487
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:074
PHP "phpinfo()" Cross-Site Scripting and Security Bypass - Advisories - Secunia	Exploit Patch Vendor Advisory web.archive.org text/html	SECUNIA 19599
PHP: PHP 5.1.3 Release Announcement	us.php.net text/html	CONFIRM us.php.net/releases/5_1_3.php
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-copy-safemode-bypass(25706)
Mandriva update for php - Advisories - Secunia	web.archive.org text/html	SECUNIA 19775
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060718 new shell bypass safe mode

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	Php	Php	4.0	All	All	All
Application	Php	Php	4.0	beta1	All	All
Application	Php	Php	4.0	beta2	All	All
Application	Php	Php	4.0	beta3	All	All
Application	Php	Php	4.0	beta4	All	All
Application	Php	Php	4.0	beta_4_patch1	All	All
Application	Php	Php	4.0	rc1	All	All
Application	Php	Php	4.0	rc2	All	All

Application	Php	Php	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All

Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta1	All	All
Application	Php	Php	5.0.0	beta2	All	All
Application	Php	Php	5.0.0	beta3	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.0	rc1	All	All
Application	Php	Php	5.0.0	rc2	All	All
Application	Php	Php	5.0.0	rc3	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.0.4	All	All	All
Application	Php	Php	5.0.5	All	All	All
Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.1.2	All	All	All
Application	Php	Php	4.0	All	All	All
Application	Php	Php	4.0	beta1	All	All
Application	Php	Php	4.0	beta2	All	All
Application	Php	Php	4.0	beta3	All	All
Application	Php	Php	4.0	beta4	All	All
Application	Php	Php	4.0	beta_4_patch1	All	All
Application	Php	Php	4.0	rc1	All	All
Application	Php	Php	4.0	rc2	All	All
Application	Php	Php	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All

Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All

Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta1	All	All
Application	Php	Php	5.0.0	beta2	All	All
Application	Php	Php	5.0.0	beta3	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.0	rc1	All	All
Application	Php	Php	5.0.0	rc2	All	All
Application	Php	Php	5.0.0	rc3	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.0.4	All	All	All
Application	Php	Php	5.0.5	All	All	All
Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.1.2	All	All	All
cpe:2.3:a:php:php:4.0:*****:						
cpe:2.3:a:php:php:4.0:beta1:*****:						
cpe:2.3:a:php:php:4.0:beta2:*****:						
cpe:2.3:a:php:php:4.0:beta3:*****:						
cpe:2.3:a:php:php:4.0:beta4:*****:						
cpe:2.3:a:php:php:4.0:beta_4_patch1:*****:						
cpe:2.3:a:php:php:4.0:rc1:*****:						
cpe:2.3:a:php:php:4.0:rc2:*****:						
cpe:2.3:a:php:php:4.0.0:*****:						
cpe:2.3:a:php:php:4.0.1:*****:						
cpe:2.3:a:php:php:4.0.1:patch1:*****:						
cpe:2.3:a:php:php:4.0.1:patch2:*****:						
cpe:2.3:a:php:php:4.0.2:*****:						
cpe:2.3:a:php:php:4.0.3:*****:						
cpe:2.3:a:php:php:4.0.3:patch1:*****:						
cpe:2.3:a:php:php:4.0.4:*****:						

.
cpe:2.3:a:php:php:4.0.4:patch1:*****:
cpe:2.3:a:php:php:4.0.5:*****:
cpe:2.3:a:php:php:4.0.6:*****:
cpe:2.3:a:php:php:4.0.7:*****:
cpe:2.3:a:php:php:4.0.7:rc1:*****:
cpe:2.3:a:php:php:4.0.7:rc2:*****:
cpe:2.3:a:php:php:4.0.7:rc3:*****:
cpe:2.3:a:php:php:4.1.0:*****:
cpe:2.3:a:php:php:4.1.1:*****:
cpe:2.3:a:php:php:4.1.2:*****:
cpe:2.3:a:php:php:4.2*:dev:*****:
cpe:2.3:a:php:php:4.2.0:*****:
cpe:2.3:a:php:php:4.2.1:*****:
cpe:2.3:a:php:php:4.2.2:*****:
cpe:2.3:a:php:php:4.2.3:*****:
cpe:2.3:a:php:php:4.3.0:*****:
cpe:2.3:a:php:php:4.3.1:*****:
cpe:2.3:a:php:php:4.3.10:*****:
cpe:2.3:a:php:php:4.3.11:*****:
cpe:2.3:a:php:php:4.3.2:*****:
cpe:2.3:a:php:php:4.3.3:*****:
cpe:2.3:a:php:php:4.3.4:*****:
cpe:2.3:a:php:php:4.3.5:*****:
cpe:2.3:a:php:php:4.3.6:*****:
cpe:2.3:a:php:php:4.3.7:*****:
cpe:2.3:a:php:php:4.3.8:*****:
cpe:2.3:a:php:php:4.3.9:*****:
cpe:2.3:a:php:php:4.4.0:*****:

cpe:2.3:a:php:php:4.4.1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.1.1:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.1.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:beta1:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:beta2:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:beta3:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:beta4:*:*:*:*:*:

cpe:2.3:a:php:php:4.0:beta_4_patch1:*:*:*:*:*

```
cpe:2.3:a:php:php:4.0:rc1:*:*:*:*:*:
```

ՀԱՅԿ ԶԳՆԻՆԻՆԻՎ ՈՐԾ.***.***.

УРЕ.2.3.а.рп.р.4.0.102.

```
cpe:2.3:a:php:php:4.0.0:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.1:patch1:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.1:patch2:*:*:*:*:*:
```

cpe:2.3:a:php:php:4.0.2:*:*:*:*:*:

```
cpe:2.3:a:php:php:4.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.3:patch1:*.:.:.:.:
```

```
cpe:2.3:a:php:php:4.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.4:patch1:*.:.:.:.:
```

```
cpe:2.3:a:php:php:4.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.0.6:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:4.0.7:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc1:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc2:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc3:*:*:*:*:*:

```
cpe:2.3:a:php:php:4.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.2:*:dev:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.2.0:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:4.2.1:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.3:*:*:*:*:*:*:

```
cpe:2.3:a:php:php:4.3.0:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:4.3.1:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:4.3.10:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.11:::*:*:*:*:*:

```
cpe:2.3:a:php:php:4.3.2:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.4:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.5:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.1:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.2:*:*:*:*:*:*:

← 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](#)