



CVE-2005-3391

Published on: 11/01/2005 12:00:00 AM UTC

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

CVE-2005-3391

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

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

Multiple vulnerabilities in PHP before 4.4.1 allow remote attackers to bypass safe_mode and open_basedir restrictions via unknown attack vectors in (1) ext/curl and (2) ext/gd.

CVE-2005-3391 has been assigned by [M](#) cve@mitre.org 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

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-4320](#)

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

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

[SECUNIA 19064](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 20898](#)

Inactive Link Not Archived

Secunia - Advisories - SUSE update for php4/php5

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

[SECUNIA 18054](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-0791](#)

SecurityReason

[securityreason.com](#)

[SREASON 525](#)

	text/html	
Secunia - Advisories - Mandriva update for php	web.archive.org text/html	 SECUNIA 18763
PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities	cve.report (archive) text/html	 BID 15411
IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	 HP SSRT061238
OpenPKG: Security Advisory [OpenPKG-SA-2005.027-php]	www.openpkg.org text/html	 OPENPKG OpenPKG-SA-2005.027
APPLE-SA-2006-03-01 Security Update 2006-001	lists.apple.com text/html	 APPLE APPLE-SA-2006-03-01
HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22691
Apple Mac OS X Security Update 2006-001 Multiple Vulnerabilities	cve.report (archive) text/html	 BID 16907
usn/usn-232-1 - Ubuntu Linux	www.ubuntu.com text/html	 UBUNTU USN-232-1
Secunia - Advisories - PHP Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 17371
Secunia - Advisories - Gentoo update for php	web.archive.org text/html	 SECUNIA 17510
Advisories - Mandriva	wwwnew.mandriva.com text/html	 MANDRIVA MDKSA-2006:035
SecurityFocus	www.securityfocus.com text/html	 SUSE SUSE-SA:2005:069
PHP: PHP 4.4.1 Release Announcement	Patch www.php.net text/html	 CONFIRM www.php.net/release_4_4_1.php
Secunia - Advisories - Ubuntu update for php4/php5	web.archive.org text/html	 SECUNIA 18198
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA-200511-08
About Security Update 2006-001	web.archive.org text/html Inactive Link Not Archived	 CONFIRM docs.info.apple.com/article.html?artnum=303382
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2005-2254
US-CERT Technical Cyber Security Alert TA06-062A -- Apple Mac Products are Affected by Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	 CERT TA06-062A

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	3.0	All	All	All
Application	Php	Php	3.0.1	All	All	All
Application	Php	Php	3.0.10	All	All	All
Application	Php	Php	3.0.11	All	All	All
Application	Php	Php	3.0.12	All	All	All
Application	Php	Php	3.0.13	All	All	All
Application	Php	Php	3.0.14	All	All	All
Application	Php	Php	3.0.15	All	All	All
Application	Php	Php	3.0.16	All	All	All
Application	Php	Php	3.0.17	All	All	All
Application	Php	Php	3.0.18	All	All	All
Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	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	4.0.5	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	3.0	All	All	All
Application	Php	Php	3.0.1	All	All	All
Application	Php	Php	3.0.10	All	All	All
Application	Php	Php	3.0.11	All	All	All
Application	Php	Php	3.0.12	All	All	All
Application	Php	Php	3.0.13	All	All	All
Application	Php	Php	3.0.14	All	All	All
Application	Php	Php	3.0.15	All	All	All
Application	Php	Php	3.0.16	All	All	All
Application	Php	Php	3.0.17	All	All	All
Application	Php	Php	3.0.18	All	All	All
Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All

Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	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	4.0.5	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
cpe:2.3:a:php:php:3.0:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.1:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.10:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.11:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.12:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.13:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.14:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.15:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.16:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.17:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.18:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.2:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.3:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.4:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.5:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.6:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.7:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.8:*:*:*:*:*:						
cpe:2.3:a:php:php:3.0.9:*:*:*:*:*:						
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:4.0.5:*:*:*:*:*:
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:3.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.1:.*:.*:.*:.*:.*:.*:.*

cpe:2.3:a:php:php:3.0.10:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.11:::*:*:*:*:*:

cpe:2.3:a:php:php:3.0.12:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.13:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.14:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.15:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.16:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.17:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.18:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.2:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.3:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.4:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.5:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.6:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.7:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.8:*:*:*:*:*:*:

cpe:2.3:a:php:php:3.0.9:*:*:*:*:*:*:

```
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:4.0.5:*****:
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:*****:

© [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](#)