



Published on: 10/31/2005 12:00:00 AM UTC

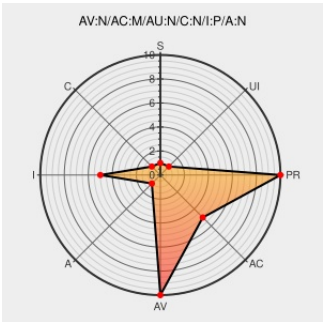
Last Modified on: 03/23/2021 11:27:23 PM UTC

# CVE-2005-3388

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of `Php` from `Php` contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the `phpinfo` function in PHP 4.x up to 4.4.0 and 5.x up to 5.0.5 allows remote attackers to inject arbitrary web script or HTML via a crafted URL with a "stacked array assignment."

CVE-2005-3388 has been assigned by  [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| NETWORK                | MEDIUM            | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| NONE                   | PARTIAL           | NONE                |

## CVE References

| Description                                                     | Tags                                                                                                 | Link                                                                                                                                                                                               |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Webmail : Solution de messagerie professionnelle - OVHcloud-OVH | <a href="#">www.vupen.com</a><br><a href="#">text/html</a>                                           |  <a href="#">VUPEN ADV-2006-4320</a>                                                                          |
| 1. Overview:                                                    | <a href="#">support.avaya.com</a><br><a href="#">text/html</a>                                       |  <a href="#">CONFIRM</a><br><a href="#">support.avaya.com/elmodocs2/security/ASA-2006-037.htm</a>             |
| SecurityFocus                                                   | <a href="#">www.securityfocus.com</a><br><a href="#">text/html</a>                                   |  <a href="#">BUGTRAQ 20051031 Advisory 18/2005: PHP Cross Site Scripting (XSS) Vulnerability in phpinfo()</a> |
| Hardened-PHP Project - PHP Security - Advisory 18/2005          | <a href="#">Vendor Advisory</a><br><a href="#">www.hardened-php.net</a><br><a href="#">text/html</a> |  <a href="#">MISC</a> <a href="#">www.hardened-php.net/advisory_182005.77.html</a>                            |
| Security Announcement                                           | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                         |  <a href="#">SUSE SUSE-SR:2005:027</a>                                                                        |

|                                                                                                                                                                   |                                                                                                                            |                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                   | <a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                                 |                                                                                                                                                |
| SecurityTracker.com Archives - PHP Input Validation Hole in phpinfo() in Processing Stacked Array Contents Lets Remote Users Conduct Cross-Site Scripting Attacks | <a href="#">securitytracker.com</a><br><a href="#">text/html</a>                                                           |  SECTRAK 1015130                                            |
| IT Resource Center - login / register                                                                                                                             | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  HP SSRT061238                                              |
| Advisories - Mandriva                                                                                                                                             | <a href="#">www.mandriva.com</a><br><a href="#">text/html</a>                                                              |  MANDRIVA MDKSA-2005:213                                    |
| OpenPKG: Security Advisory [OpenPKG-SA-2005.027-php]                                                                                                              | <a href="#">www.openpkg.org</a><br><a href="#">text/html</a>                                                               |  OPENPKG OpenPKG-SA-2005.027                                |
| rhn.redhat.com   Red Hat Support                                                                                                                                  | <a href="#">www.redhat.com</a><br><a href="#">text/html</a>                                                                |  REDHAT RHSA-2005:838                                       |
| rhn.redhat.com   Red Hat Support                                                                                                                                  | <a href="#">www.redhat.com</a><br><a href="#">text/html</a>                                                                |  REDHAT RHSA-2005:831                                       |
| Secunia - Advisories - Fedora update for php                                                                                                                      | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 17490                                              |
| PHP PHPInfo Cross-Site Scripting Vulnerability                                                                                                                    | <a href="#">Patch</a><br><a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                 |  BID 15248                                                  |
| Red Hat Stronghold updates for uw-imap and PHP - Advisories - Secunia                                                                                             | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 21252                                              |
| HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia                                                                                 | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 22691                                            |
| usn/usn-232-1 - Ubuntu Linux                                                                                                                                      | <a href="#">www.ubuntu.com</a><br><a href="#">text/html</a>                                                                |  UBUNTU USN-232-1                                         |
| Secunia - Advisories - SUSE Updates for Multiple Packages                                                                                                         | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 17559                                            |
| Secunia - Advisories - PHP Multiple Vulnerabilities                                                                                                               | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a>   |  SECUNIA 17371                                            |
| Secunia - Advisories - Gentoo update for php                                                                                                                      | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 17510                                            |
| rhn.redhat.com   Red Hat Support                                                                                                                                  | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  REDHAT RHSA-2006:0549                                    |
| The Fedora Legacy Project                                                                                                                                         | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  FEDORA FLSA:166943                                       |
| Secunia - Advisories - Avaya Products PHP Multiple Vulnerabilities                                                                                                | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 18669                                            |
| PHP: PHP 4.4.1 Release Announcement                                                                                                                               | <a href="#">Patch</a><br><a href="#">www.php.net</a><br><a href="#">text/html</a>                                          |  CONFIRM<br><a href="#">www.php.net/release_4_4_1.php</a> |
| Secunia - Advisories - Red Hat update for php                                                                                                                     | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                                               |  SECUNIA 17531                                            |
| 404 Not Found                                                                                                                                                     | <a href="#">www.turbolinux.com</a>                                                                                         |  TURBO TLSA-2006-38                                       |

[text/plain](#)[Inactive Link](#)[Not Archived](#)

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

Repository / Oval Repository

[oval.cisecurity.org](#)[text/html](#) OVAL oval:org.mitre.oval:def:10542

[SECURITY] Fedora 32 Update: ca-certificates-2020.2.41-1.1.fc32 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)[text/html](#) FEDORA FEDORA-2020-fb144e7de5

Secunia - Advisories - Mandriva update for php

[web.archive.org](#)[text/html](#) SECUNIA 17557

Webmail - OVH

[www.vupen.com](#)[text/html](#) VUPEN ADV-2005-2254

PHP Cross Site Scripting (XSS) Vulnerability in phpinfo() - CXSecurity.com

[securityreason.com](#)[text/html](#) SREASON 133

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](mailto: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 | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.0   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | patch1 | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | patch2 | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.2   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.3   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.3   | patch1 | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.4   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.5   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.6   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.7   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.7   | rc1    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.7   | rc2    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.7   | rc3    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.1.0   | All    | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.1.1   | 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 | 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 | 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 | 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 |
| 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:4.2.0:*:*:*:*:*:       |
| 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: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: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:4.3.5:*:*:*:*:*:       |
| 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: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:*:*:*:*:*:       |

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](#)