

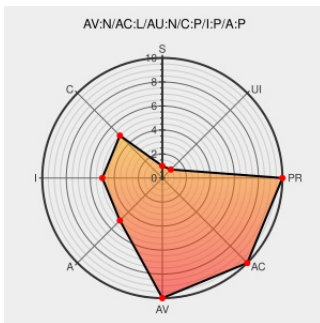


CVE-2012-1823

Published on: 05/11/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:19 PM UTC

CVE-2012-1823

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

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

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

CVE-2012-1823 has been assigned by cert@cert.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

HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Unauthorized Access, Disclosure of Information, Data Modification, Denial of Service (DoS), Execution of Arbitrary Code - c03360041 - HP Business Support Center

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[HP HPSBMU02786](#)

Red Hat Customer Portal

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2012:0570](#)

APPLE-SA-2012-09-19-2 OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security

[lists.apple.com](#)

[text/html](#)

[APPLE APPLE-SA-2012-09-19-2](#)

Update 2012-004		
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0547
About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 49085
About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT5501
Support / Security / Advisories // MDVSA-2012:068 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2012:068
PHP Command Parameter Bug Lets Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1027022
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0568
DE EINDBAZEN » Eindbazen PHP-CGI advisory (CVE-2012-1823)	Exploit eindbazen.net text/html	 MISC eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
Vulnerability Note VU#520827 - PHP-CGI query string parameter vulnerability	Exploit US Government Resource www.kb.cert.org text/html	 CERT-VN VU#520827
[security-announce] openSUSE-SU-2012:0590-1: critical: update for php5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2012:0590
Debian -- Security Information -- DSA-2465-1 php5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2465
PHP :: Bug #61910 :: Patches	bugs.php.net text/xml	 CONFIRM bugs.php.net/patch-display.php?bug_id=61910&patch=cgi.diff&revision=1335984315&display=1
Security Alerts - Secunia	web.archive.org text/html	 SECUNIA 49014
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0569
PHP: News Archive - 2012	www.php.net text/html	 CONFIRM www.php.net/archive/2012.php#id2012-05-03-1
Vulnerability Note VU#673343 - Parallels Plesk Panel phppath/php vulnerability	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#673343
'[security bulletin] HPSBUX02791 SSRT100856 rev.1 - HP-UX Apache Web Server running PHP, Remote Execu' - MARC	marc.info text/html	 HP SSRT100856
PHP :: Sec Bug #61910 :: VU#520827 - PHP-CGI query string parameter vulnerability	Exploit Patch bugs.php.net text/xml	 CONFIRM bugs.php.net/bug.php?id=61910

About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 49065
Security Alerts - Secunia	web.archive.org text/html	 SECUNIA 49087
[security-announce] SUSE-SU-2012:0604-1: critical: Security update for P	lists.opensuse.org text/html	 SUSE SUSE-SU-2012:0604
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0546
[security-announce] SUSE-SU-2012:0598-1: critical: Security update for P	lists.opensuse.org text/html	 SUSE SUSE-SU-2012:0598
PHP: PHP 5 ChangeLog	Exploit Patch www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php#5.4.2

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	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	5.1.3	All	All	All

Application	Php	Php	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	All	All	All
Application	Php	Php	5.2.15	All	All	All
Application	Php	Php	5.2.16	All	All	All
Application	Php	Php	5.2.17	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All
Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.10	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.1	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	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	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	All	All	All
Application	Php	Php	5.2.15	All	All	All
Application	Php	Php	5.2.16	All	All	All
Application	Php	Php	5.2.17	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All

Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.10	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.4	All	All	All
Application	Php	Php	5.3.5	All	All	All
Application	Php	Php	5.3.6	All	All	All
Application	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.8	All	All	All
Application	Php	Php	5.3.9	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	5.4.1	All	All	All
Application	Php	Php	All	All	All	All
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:5.1.3:*****:
cpe:2.3:a:php:php:5.1.4:*****:
cpe:2.3:a:php:php:5.1.5:*****:
cpe:2.3:a:php:php:5.1.6:*****:
cpe:2.3:a:php:php:5.2.0:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.2.10:*****:
cpe:2.3:a:php:php:5.2.11:*****:
cpe:2.3:a:php:php:5.2.12:*****:
cpe:2.3:a:php:php:5.2.13:*****:
cpe:2.3:a:php:php:5.2.14:*****:
cpe:2.3:a:php:php:5.2.15:*****:
cpe:2.3:a:php:php:5.2.16:*****:
cpe:2.3:a:php:php:5.2.17:*****:
cpe:2.3:a:php:php:5.2.2:*****:
cpe:2.3:a:php:php:5.2.3:*****:
cpe:2.3:a:php:php:5.2.4:*****:
cpe:2.3:a:php:php:5.2.5:*****:
cpe:2.3:a:php:php:5.2.6:*****:
cpe:2.3:a:php:php:5.2.7:*****:
cpe:2.3:a:php:php:5.2.8:*****:
cpe:2.3:a:php:php:5.2.9:*****:
cpe:2.3:a:php:php:5.3.0:*****:
cpe:2.3:a:php:php:5.3.1:*****:
cpe:2.3:a:php:php:5.3.10:*****:
cpe:2.3:a:php:php:5.3.2:*****:
cpe:2.3:a:php:php:5.3.3:*****:
cpe:2.3:a:php:php:5.3.4:*****:

cpe:2.3:a:php:php:5.3.5:*****:
cpe:2.3:a:php:php:5.3.6:*****:
cpe:2.3:a:php:php:5.3.7:*****:
cpe:2.3:a:php:php:5.3.8:*****:
cpe:2.3:a:php:php:5.3.9:*****:
cpe:2.3:a:php:php:5.4.0:*****:
cpe:2.3:a:php:php:5.4.1:*****:
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:5.1.3:*****:
cpe:2.3:a:php:php:5.1.4:*****:
cpe:2.3:a:php:php:5.1.5:*****:
cpe:2.3:a:php:php:5.1.6:*****:
cpe:2.3:a:php:php:5.2.0:*****:
cpe:2.3:a:php:php:5.2.1:*****:


```
cpe:/a:prip:prip:5.2.1 : : : : :
```

cpe:2.3:a:php:php:5.2.10:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.11:::*:*:*:*:*:

cpe:2.3:a:php:php:5.2.12:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.13:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.14:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.15:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.16:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.17:*:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.2.3:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.2.4:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.2.5:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.2.6:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.2.7:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.8:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.9:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:
```

```
cpe:2.3:a:php:php:5.3.10:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:

```
cpe:2.3:a:php:php:5.4.0:*:*:*:*:*:*:
```

cpe:2.3:a:php:php:5.4.1:*****:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/hacking	Penetration Test Laboratories [Vulnerable VM's, Web App's]	2014-05-10 02:08:14
 /r/netsecstudents	Penetration Test Laboratories [VM's]	2014-05-10 00:09:19

← Previous ID

Next ID→