

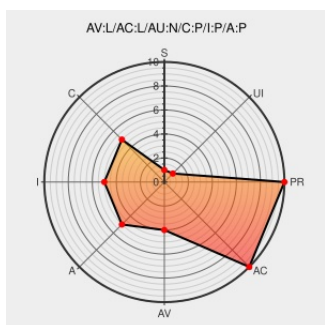


CVE-2014-4670

Published on: 07/10/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4670

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

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

Use-after-free vulnerability in ext/spl/spl_dlist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-hosting environments.

CVE-2014-4670 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Security Advisory SA54553 - SUSE update for php5 - Secunia

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

[SECUNIA 54553](#)

Oracle Bulletin Board Update - January 2015

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#)
[www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2014:1765](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2014:1326](#)

openSUSE-SU-2014:0945-1: moderate: php5: security fixes

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2014:0945](#)

About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 59831
APPLE-SA-2015-04-08-2 OS X 10.10.3 and Security Update 2015-004	lists.apple.com text/html	 APPLE APPLE-SA-2015-04-08-2
openSUSE-SU-2014:1236-1: moderate: several security fixes for php5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:1236
PHP :: Bug #67538 :: SPL Iterators use-after-free	bugs.php.net text/html	 CONFIRM bugs.php.net/bug.php?id=67538
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:1327
Security Advisory SA60696 - Debian update for php5 - Secunia	web.archive.org text/html	 SECUNIA 60696
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:1766
IBM Security Bulletin: Multiple vulnerabilities in PHP 5.2 open source component for IBM Lotus Protector for Mail Security (CVE-2014-3515 CVE-2014-4049 CVE-2014-3981 CVE-2014-0238 CVE-2014-0237, CVE-2014-4721, CVE-2014-4670 CVE-2014-4698) - United States	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21683486
Debian -- Security Information -- DSA-3008-1 php5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3008
About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004 - Apple Support	support.apple.com text/html	 CONFIRM support.apple.com/HT204659

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	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All

Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All

Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	All	All	All	All
cpe:2.3:a:php:php:5.5.0:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha3:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha4:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha5:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:alpha6:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:beta1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:beta2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:beta3:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:beta4:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.0:rc2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.10:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.11:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.12:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.13:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.5.3:*:*:*:*:*:						

cpe:2.3:a:php:php:5.5.4:*****:
cpe:2.3:a:php:php:5.5.5:*****:
cpe:2.3:a:php:php:5.5.6:*****:
cpe:2.3:a:php:php:5.5.7:*****:
cpe:2.3:a:php:php:5.5.8:*****:
cpe:2.3:a:php:php:5.5.9:*****:
cpe:2.3:a:php:php:5.5.0:*****:
cpe:2.3:a:php:php:5.5.0:alpha1:*****:
cpe:2.3:a:php:php:5.5.0:alpha2:*****:
cpe:2.3:a:php:php:5.5.0:alpha3:*****:
cpe:2.3:a:php:php:5.5.0:alpha4:*****:
cpe:2.3:a:php:php:5.5.0:alpha5:*****:
cpe:2.3:a:php:php:5.5.0:alpha6:*****:
cpe:2.3:a:php:php:5.5.0:beta1:*****:
cpe:2.3:a:php:php:5.5.0:beta2:*****:
cpe:2.3:a:php:php:5.5.0:beta3:*****:
cpe:2.3:a:php:php:5.5.0:beta4:*****:
cpe:2.3:a:php:php:5.5.0:rc1:*****:
cpe:2.3:a:php:php:5.5.0:rc2:*****:
cpe:2.3:a:php:php:5.5.1:*****:
cpe:2.3:a:php:php:5.5.10:*****:
cpe:2.3:a:php:php:5.5.11:*****:
cpe:2.3:a:php:php:5.5.12:*****:
cpe:2.3:a:php:php:5.5.13:*****:
cpe:2.3:a:php:php:5.5.2:*****:
cpe:2.3:a:php:php:5.5.3:*****:
cpe:2.3:a:php:php:5.5.4:*****:
cpe:2.3:a:php:php:5.5.5:*****:

cpe:2.3:a:php:php:5.5.6:*:*:*:*:*
cpe:2.3:a:php:php:5.5.7:*:*:*:*:*
cpe:2.3:a:php:php:5.5.8:*:*:*:*:*
cpe:2.3:a:php:php:5.5.9:*:*:*:*:*
cpe:2.3:a:php:php:*:*:*:*:*:

cpe:2.3:a:php:php:5.5.6:*:*:*:*:*:
cpe:2.3:a:php:php:5.5.7:*:*:*:*:*:
cpe:2.3:a:php:php:5.5.8:*:*:*:*:*:
cpe:2.3:a:php:php:5.5.9:*:*:*:*:*:
cpe:2.3:a:php:php:*:*:*:*:*:

cpe:2.3:a:php:php:5.5.6:*:*:*:*:*
cpe:2.3:a:php:php:5.5.7:*:*:*:*:*
cpe:2.3:a:php:php:5.5.8:*:*:*:*:*
cpe:2.3:a:php:php:5.5.9:*:*:*:*:*
cpe:2.3:a:php:php:*:*:*:*:*:

cpe:2.3:a:php:php:5.5.6:*:*:*:*:*
cpe:2.3:a:php:php:5.5.7:*:*:*:*:*
cpe:2.3:a:php:php:5.5.8:*:*:*:*:*
cpe:2.3:a:php:php:5.5.9:*:*:*:*:*
cpe:2.3:a:php:php:*:*:*:*:*:

cpe:2.3:a:php:php:5.5.6:*:*:*:*:*
cpe:2.3:a:php:php:5.5.7:*:*:*:*:*
cpe:2.3:a:php:php:5.5.8:*:*:*:*:*
cpe:2.3:a:php:php:5.5.9:*:*:*:*:*
cpe:2.3:a:php:php:*:*:*:*:*:

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