



CVE-2014-5120

Published on: 08/22/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

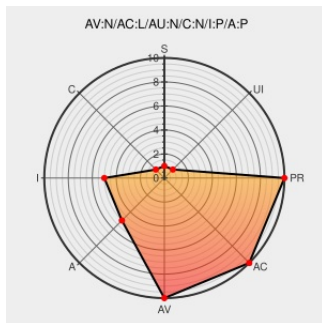
CVE-2014-5120

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Php](#) from [Php](#) contain the following vulnerability: `gd_ctx.c` in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack `%00` sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) `imagegd`, (2) `imagegd2`, (3) `imagegif`, (4) `imagejpeg`, (5) `imagepng`, (6) `imagewbmp`, or (7) `imagewebp` function.

CVE-2014-5120 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

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

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

PHP :: Sec Bug #67730 :: CVE-2014-5120 Null byte injection possible with `imagexxx` functions

[Vendor Advisory](#)

[bugs.php.net](#)

[text/html](#)

CONFIRM bugs.php.net/bug.php?id=67730

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:132/
openSUSE-SU-2014:1133-1: moderate: php5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:1133
PHP: PHP 5 ChangeLog	php.net text/html	 CONFIRM php.net/ChangeLog-5.php
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:1766
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	5.4.0	All	All	All
Application	Php	Php	5.4.0	beta2	All	All
Application	Php	Php	5.4.0	beta2	32-bit	All
Application	Php	Php	5.4.0	rc2	All	All
Application	Php	Php	5.4.1	All	All	All
Application	Php	Php	5.4.10	All	All	All
Application	Php	Php	5.4.11	All	All	All
Application	Php	Php	5.4.12	All	All	All
Application	Php	Php	5.4.12	rc1	All	All
Application	Php	Php	5.4.12	rc2	All	All
Application	Php	Php	5.4.13	All	All	All
Application	Php	Php	5.4.13	rc1	All	All
Application	Php	Php	5.4.14	All	All	All
Application	Php	Php	5.4.14	rc1	All	All
Application	Php	Php	5.4.15	All	All	All
Application	Php	Php	5.4.15	rc1	All	All
Application	Php	Php	5.4.16	rc1	All	All
Application	Php	Php	5.4.17	All	All	All
Application	Php	Php	5.4.18	All	All	All

Application	Php	Php	5.4.19	All	All	All
Application	Php	Php	5.4.2	All	All	All
Application	Php	Php	5.4.20	All	All	All
Application	Php	Php	5.4.21	All	All	All
Application	Php	Php	5.4.22	All	All	All
Application	Php	Php	5.4.23	All	All	All
Application	Php	Php	5.4.24	All	All	All
Application	Php	Php	5.4.25	All	All	All
Application	Php	Php	5.4.26	All	All	All
Application	Php	Php	5.4.27	All	All	All
Application	Php	Php	5.4.28	All	All	All
Application	Php	Php	5.4.29	All	All	All
Application	Php	Php	5.4.3	All	All	All
Application	Php	Php	5.4.30	All	All	All
Application	Php	Php	5.4.31	All	All	All
Application	Php	Php	5.4.4	All	All	All
Application	Php	Php	5.4.5	All	All	All
Application	Php	Php	5.4.6	All	All	All
Application	Php	Php	5.4.7	All	All	All
Application	Php	Php	5.4.8	All	All	All
Application	Php	Php	5.4.9	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	5.5.14	All	All	All
Application	Php	Php	5.5.15	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	5.4.0	All	All	All
Application	Php	Php	5.4.0	beta2	All	All
Application	Php	Php	5.4.0	beta2	32-bit	All
Application	Php	Php	5.4.0	rc2	All	All
Application	Php	Php	5.4.1	All	All	All
Application	Php	Php	5.4.10	All	All	All
Application	Php	Php	5.4.11	All	All	All
Application	Php	Php	5.4.12	All	All	All
Application	Php	Php	5.4.12	rc1	All	All
Application	Php	Php	5.4.12	rc2	All	All
Application	Php	Php	5.4.13	All	All	All
Application	Php	Php	5.4.13	rc1	All	All
Application	Php	Php	5.4.14	All	All	All
Application	Php	Php	5.4.14	rc1	All	All
Application	Php	Php	5.4.15	All	All	All
Application	Php	Php	5.4.15	rc1	All	All
Application	Php	Php	5.4.16	rc1	All	All
Application	Php	Php	5.4.17	All	All	All
Application	Php	Php	5.4.18	All	All	All
Application	Php	Php	5.4.19	All	All	All
Application	Php	Php	5.4.2	All	All	All

Application	Php	Php	5.4.20	All	All	All
Application	Php	Php	5.4.21	All	All	All
Application	Php	Php	5.4.22	All	All	All
Application	Php	Php	5.4.23	All	All	All
Application	Php	Php	5.4.24	All	All	All
Application	Php	Php	5.4.25	All	All	All
Application	Php	Php	5.4.26	All	All	All
Application	Php	Php	5.4.27	All	All	All
Application	Php	Php	5.4.28	All	All	All
Application	Php	Php	5.4.29	All	All	All
Application	Php	Php	5.4.3	All	All	All
Application	Php	Php	5.4.30	All	All	All
Application	Php	Php	5.4.31	All	All	All
Application	Php	Php	5.4.4	All	All	All
Application	Php	Php	5.4.5	All	All	All
Application	Php	Php	5.4.6	All	All	All
Application	Php	Php	5.4.7	All	All	All
Application	Php	Php	5.4.8	All	All	All
Application	Php	Php	5.4.9	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	5.5.14	All	All	All
Application	Php	Php	5.5.15	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
cpe:2.3:a:php:php:5.4.0:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.0:beta2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.0:beta2:32-bit:*:*:*:*:						
cpe:2.3:a:php:php:5.4.0:rc2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.10:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.11:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.12:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.12:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.12:rc2:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.13:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.13:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.14:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.14:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.15:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.15:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.16:rc1:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.17:*:*:*:*:*:						
cpe:2.3:a:php:php:5.4.18:*:*:*:*:*:						

cpe:2.3:a:php:php:5.4.19:*****:
cpe:2.3:a:php:php:5.4.2:*****:
cpe:2.3:a:php:php:5.4.20:*****:
cpe:2.3:a:php:php:5.4.21:*****:
cpe:2.3:a:php:php:5.4.22:*****:
cpe:2.3:a:php:php:5.4.23:*****:
cpe:2.3:a:php:php:5.4.24:*****:
cpe:2.3:a:php:php:5.4.25:*****:
cpe:2.3:a:php:php:5.4.26:*****:
cpe:2.3:a:php:php:5.4.27:*****:
cpe:2.3:a:php:php:5.4.28:*****:
cpe:2.3:a:php:php:5.4.29:*****:
cpe:2.3:a:php:php:5.4.3:*****:
cpe:2.3:a:php:php:5.4.30:*****:
cpe:2.3:a:php:php:5.4.31:*****:
cpe:2.3:a:php:php:5.4.4:*****:
cpe:2.3:a:php:php:5.4.5:*****:
cpe:2.3:a:php:php:5.4.6:*****:
cpe:2.3:a:php:php:5.4.7:*****:
cpe:2.3:a:php:php:5.4.8:*****:
cpe:2.3:a:php:php:5.4.9:*****:
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:5.5.14:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.5.15:~::~~::~~::~~:::
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:5.4.0:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.0:beta2:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.0:beta2:32-bit:~::~~::~~:::
cpe:2.3:a:php:php:5.4.0:rc2:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.1:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.10:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.11:~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.12:~::~~::~~::~~:::

cpe:2.3:a:php:php:5.4.12:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.12:rc2:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.13:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.13:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.14:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.14:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.15:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.15:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.16:rc1:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.17:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.18:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.19:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.2:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.20:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.21:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.22:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.23:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.24:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.25:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.26:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.27:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.28:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.29:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.3:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.30:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.31:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.4:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.5:~::~~::~~::~~::~~::~~:::
cpe:2.3:a:php:php:5.4.6:~::~~::~~::~~::~~::~~:::

cpe:2.3:a:php:php:5.4.7:*****:
cpe:2.3:a:php:php:5.4.8:*****:
cpe:2.3:a:php:php:5.4.9:*****:
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:5.5.14:*****:
cpe:2.3:a:php:php:5.5.15:*****:
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:*****:

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](#)