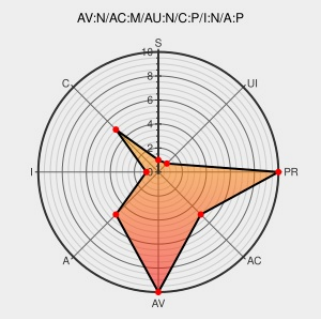
CVE-2013-7328

Published on: 02/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7328

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Php from Php contain the following vulnerability:

Multiple integer signedness errors in the gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 allow remote attackers to cause a denial of service (application crash) or obtain sensitive information via an imagecrop function call with a negative value for the (1) x or (2) y dimension, a different vulnerability than CVE-2013-7226.

CVE-2013-7328 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
Bug 1065108 – CVE-2013-7226 CVE-2013-7327 CVE-2013-7328 CVE-2014-2020 php: multiple vulnerabilities in gdImageCrop()	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1065108
PHP :: Sec Bug #66356 :: Heap Overflow Vulnerability in imagecrop()	Vendor Advisory bugs.php.net text/xml	CONFIRM bugs.php.net/bug.php?id=66356
208.43.231.11 Git - php-src.git/commit	Vendor Advisory git.php.net text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=8f4a5373bb71590352fd934028d6dde5bc18530b
USN-2126-1: PHP vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2126-1

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	5.5.2	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	5.5.0	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	5.5.2	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

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:5.5.2:*:*:*:*:*:*:*:

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:5.5.0:*:*:*:*:*:*:*:

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:5.5.2:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report