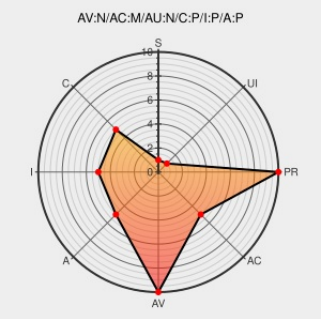
CVE-2013-7327

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

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

CVE-2013-7327

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check return values, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via invalid imagecrop arguments that lead to use of a NULL pointer as a return value, a different vulnerability than CVE-2013-7226.

CVE-2013-7327 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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()	Issue Tracking, Third Party Advisory, VDB Entry, 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	Patch, git.php.net, text/xml	CONFIRM git.php.net/?p=php-src.git;a=commit;h=8f4a5373bb71590352fd934028d6dde5bc18530b

USN-2126-1: PHP vulnerabilities | Ubuntu

Third Party Advisory
www.ubuntu.com
text/html

UBUNTU USN-2126-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	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	5.5.0	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	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→