

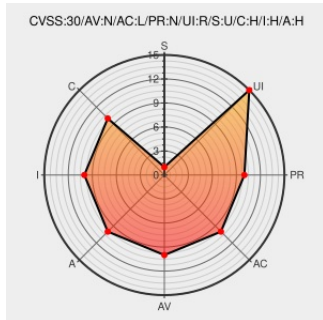


CVE-2016-5767

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5767

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

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

Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.

CVE-2016-5767 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

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
PHP CVE-2016-5767 Integer Overflow Vulnerability	cve.report (archive) text/html	BID 91395
openSUSE-SU-2016-1922-1: moderate	lists.opensuse.org	SUSE openSUSE-SU-2016-1922

openSUSE SU-2016:1722-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE SU-2016:1722
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2598
Document Display HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
PHP: PHP 7 ChangeLog	Release Notes php.net text/html	CONFIRM php.net/ChangeLog-7.php
[security-announce] SUSE-SU-2016:2013-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2013
oss-security - Re: CVE for PHP 5.5.37 issues	Release Notes www.openwall.com text/html	MLIST [oss-security] 20160623 Re: CVE for PHP 5.5.37 issues
PHP :: Sec Bug #72446 :: Integer Overflow in gdImagePaletteToTrueColor() resulting in heap overflow	bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=72446
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
iFixed bug #72446 - Integer Overflow in gdImagePaletteToTrueColor() r... · php/php-src@c395c6e · GitHub	github.com text/html	CONFIRM github.com/php/php-src/commit/c395c6e5d7e8df37a21265ff76e48fe75ceb5ae6?w=1
PHP: PHP 5 ChangeLog	Release Notes php.net text/html	CONFIRM php.net/ChangeLog-5.php
[security-announce] openSUSE-SU-2016:1761-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1761

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	Libgd	Libgd	All	All	All	All
Application	Php	Php	5.6.0	alpha1	All	All
Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All

Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	5.6.0	alpha1	All	All

Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.13	All	All	All
Application	Php	Php	5.6.14	All	All	All
Application	Php	Php	5.6.15	All	All	All
Application	Php	Php	5.6.16	All	All	All
Application	Php	Php	5.6.17	All	All	All
Application	Php	Php	5.6.18	All	All	All
Application	Php	Php	5.6.19	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.20	All	All	All
Application	Php	Php	5.6.21	All	All	All
Application	Php	Php	5.6.22	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All

Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	All	All	All	All
cpe:2.3:a:libgd:libgd:*:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:alpha1:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:alpha2:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:alpha3:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:alpha4:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:alpha5:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:beta1:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:beta2:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:beta3:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.0:beta4:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.1:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.10:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.11:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.12:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.13:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.14:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.15:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.16:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.17:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.18:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.19:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.2:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.20:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.21:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.22:*:*:*:*.*						
cpe:2.3:a:php:php:5.6.3:*:*:*:*.*						

cpe:2.3:a:php:php:5.6.4:*****:
cpe:2.3:a:php:php:5.6.5:*****:
cpe:2.3:a:php:php:5.6.6:*****:
cpe:2.3:a:php:php:5.6.7:*****:
cpe:2.3:a:php:php:5.6.8:*****:
cpe:2.3:a:php:php:5.6.9:*****:
cpe:2.3:a:php:php:7.0.0:*****:
cpe:2.3:a:php:php:7.0.1:*****:
cpe:2.3:a:php:php:7.0.2:*****:
cpe:2.3:a:php:php:7.0.3:*****:
cpe:2.3:a:php:php:7.0.4:*****:
cpe:2.3:a:php:php:7.0.5:*****:
cpe:2.3:a:php:php:7.0.6:*****:
cpe:2.3:a:php:php:7.0.7:*****:
cpe:2.3:a:php:php:*****:
cpe:2.3:a:php:php:5.6.0:alpha1:*****:
cpe:2.3:a:php:php:5.6.0:alpha2:*****:
cpe:2.3:a:php:php:5.6.0:alpha3:*****:
cpe:2.3:a:php:php:5.6.0:alpha4:*****:
cpe:2.3:a:php:php:5.6.0:alpha5:*****:
cpe:2.3:a:php:php:5.6.0:beta1:*****:
cpe:2.3:a:php:php:5.6.0:beta2:*****:
cpe:2.3:a:php:php:5.6.0:beta3:*****:
cpe:2.3:a:php:php:5.6.0:beta4:*****:
cpe:2.3:a:php:php:5.6.1:*****:
cpe:2.3:a:php:php:5.6.10:*****:
cpe:2.3:a:php:php:5.6.11:*****:
cpe:2.3:a:php:php:5.6.12:*****:

cpe:2.3:a:php:php:5.6.13:*****:
cpe:2.3:a:php:php:5.6.14:*****:
cpe:2.3:a:php:php:5.6.15:*****:
cpe:2.3:a:php:php:5.6.16:*****:
cpe:2.3:a:php:php:5.6.17:*****:
cpe:2.3:a:php:php:5.6.18:*****:
cpe:2.3:a:php:php:5.6.19:*****:
cpe:2.3:a:php:php:5.6.2:*****:
cpe:2.3:a:php:php:5.6.20:*****:
cpe:2.3:a:php:php:5.6.21:*****:
cpe:2.3:a:php:php:5.6.22:*****:
cpe:2.3:a:php:php:5.6.3:*****:
cpe:2.3:a:php:php:5.6.4:*****:
cpe:2.3:a:php:php:5.6.5:*****:
cpe:2.3:a:php:php:5.6.6:*****:
cpe:2.3:a:php:php:5.6.7:*****:
cpe:2.3:a:php:php:5.6.8:*****:
cpe:2.3:a:php:php:5.6.9:*****:
cpe:2.3:a:php:php:7.0.0:*****:
cpe:2.3:a:php:php:7.0.1:*****:
cpe:2.3:a:php:php:7.0.2:*****:
cpe:2.3:a:php:php:7.0.3:*****:
cpe:2.3:a:php:php:7.0.4:*****:
cpe:2.3:a:php:php:7.0.5:*****:
cpe:2.3:a:php:php:7.0.6:*****:
cpe:2.3:a:php:php:7.0.7:*****:
cpe:2.3:a:php:php:*****:

No vendor comments have been submitted for this CVE

© [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](#)