

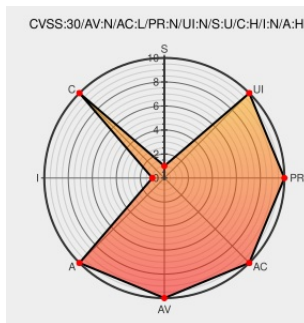


CVE-2016-1903

Published on: 01/18/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1903

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

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

The `gdImageRotateInterpolated` function in `ext/gd/libgd/gd_interpolation.c` in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large `bgd_color` argument to the `imagerotate` function.

CVE-2016-1903 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
PHP 'gd_interpolation.c' Out of Bounds Read Memory Corruption Vulnerability	cve.report (archive) text/html	🌐 BID 79916
openSUSE-SU-2016-0251-1: moderate	lists.opensuse.org	🌐 SUSE openSUSE-SU-2016-0251

openSUSE-SU-2016-0201-1: moderate: Security update for php5	lists.opensuse.org text/html	 openSUSE-SU-2016-0201-1
USN-2952-2: PHP regression Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2952-2
openSUSE-SU-2016:0366-1: moderate: Security update for php5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0366
PHP :: Bug #70976 :: Memory Read via gdImageRotateInterpolated Array Index Out of Bounds	Exploit bugs.php.net text/html	 CONFIRM bugs.php.net/bug.php?id=70976
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
The Slackware Linux Project: Slackware Security Advisories	www.slackware.com text/html	 SLACKWARE SSA:2016-034-04
oss-security - [CVE Request] Multiple PHP issues	www.openwall.com text/html	 MLIST [oss-security] 20160115 [CVE Request] Multiple PHP issues
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2750
USN-2952-1: PHP vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2952-1
PHP Bugs May Let Remote Users Obtain Potentially Sensitive Information, Gain Elevated Privileges, or Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1034608
PHP: PHP 7 ChangeLog	Vendor Advisory www.php.net text/html	 CONFIRM www.php.net/ChangeLog-7.php
PHP: PHP 5 ChangeLog	Vendor Advisory www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php

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	5.6.0	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	5.6.2	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	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	5.6.2	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	All	All	All	All
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:5.6.2:*****:
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: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:5.6.2:*****:
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:*****:

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](#)