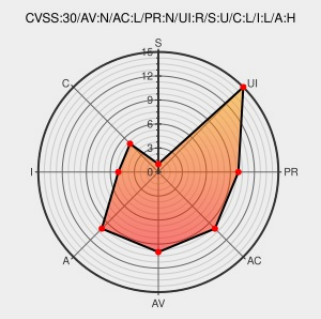
CVE-2013-7456

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

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

CVE-2013-7456

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



Certain versions of Libgd from Libgd contain the following vulnerability:

gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.

CVE-2013-7456 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	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
Debian -- Security Information -- DSA-3602-1 php5	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3602
USN-3030-1: GD library	www.ubuntu.com	UBUNTU USN-3030-1

vulnerabilities | Ubuntu	text/html	
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
Fixed memory overrun bug in gdImageScaleTwoPass · libgd/libgd@4f65a3e · GitHub	github.com text/html	CONFIRM github.com/libgd/libgd/commit/4f65a3e4eedaffa1efcf9ee1eb08f0b504fbc31a
PHP :: Sec Bug #72227 :: imagescale out-of-bounds read	Exploit bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=72227
Debian -- Security Information -- DSA-3587-1 libgd2	www.debian.org Depreciated Link text/html	DEBIAN DSA-3587
PHP 'imagescale' Function Out of Bounds Read Denial of Service Vulnerability	cve.report (archive) text/html	BID 90859
oss-security - Re: Fwd: CVE for PHP 5.5.36 issues	Release Notes www.openwall.com text/html	MLIST [oss-security] 20160526 Re: Fwd: CVE for PHP 5.5.36 issues
Fixed bug #72227: imagescale out-of-bounds read · php/php-src@7a1aac3 · GitHub	github.com text/html	CONFIRM github.com/php/php-src/commit/7a1aac3343af85b4af4df5f8844946eaa27394ab?w=1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
PHP: PHP 5 ChangeLog	Release Notes php.net text/html	CONFIRM php.net/ChangeLog-5.php

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	2.1.0	All	All	All
Application	Libgd	Libgd	2.1.0	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	5.6.3	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	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	5.6.3	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	All	All	All	All

cpe:2.3:a:libgd:libgd:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:libgd:libgd:2.1.0:*:*:*:*:*:*:*:

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:5.6.3:*:*:*:*:*:*:*:

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

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:5.6.3:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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