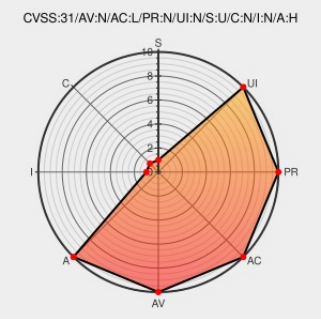
CVE-2016-6128

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

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

CVE-2016-6128

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



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

The gdImageCropThreshold function in gd_crop.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 7.0.9, allows remote attackers to cause a denial of service (application crash) via an invalid color index.

CVE-2016-6128 has been assigned by security@debian.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
GD Library gdImageCropThreshold() Out-of-Bounds Memory Read Error Lets Remote Users Cause the Target Application to Crash -	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1036276

SecurityTracker		
GD: Multiple vulnerabilities (GLSA 201612-09) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201612-09
oss-security - Re: CVE Request: libgd: Invalid color index is not properly handled leading to denial of service (crash)	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160629 Re: CVE Request: libgd: Invalid color index is not properly handled leading to denial of service (crash)
PHP :: Sec Bug #72494 :: imagecropauto out-of-bounds access	Issue Tracking Permissions Required bugs.php.net text/html	CONFIRM bugs.php.net/72494
USN-3030-1: GD library vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-3030-1
fix php 72494, invalid color index not handled, can lead to crash · libgd/libgd@6ff72ae · GitHub	Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/libgd/libgd/commit/6ff72ae40c7c20ece939afb362d98cc37f4a1c96
LibGD 2.2.3 release	Release Notes Third Party Advisory libgd.github.io text/html	CONFIRM libgd.github.io/release-2.2.3.html
openSUSE-SU-2016:2117-1: moderate: Security update for gd	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2117
libgd CVE-2016-6128 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 91509
fix php 72494, invalid color index not handled, can lead to crash · libgd/libgd@1ccfe21 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/libgd/libgd/commit/1ccfe21e14c4d18336f9da8515cd17db88c3de61
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
Debian -- Security Information -- DSA-3619-1 libgd2	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3619
openSUSE-SU-2016:2363-1: moderate: Security update for gd	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2363

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libgd	Libgd	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→