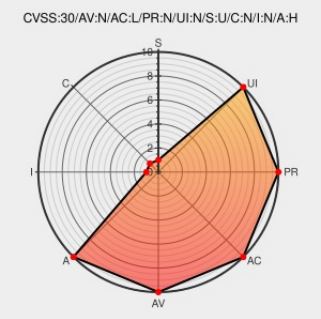
CVE-2015-8877

Published on: 05/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8877

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



Certain versions of Libgd from Libgd contain the following vulnerability:

The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.

CVE-2015-8877 has been assigned by cve@mitre.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
gdImageScaleTwoPass() can leak memory · Issue #173 · libgd/libgd · GitHub	Patch, github.com, text/html	CONFIRM github.com/libgd/libgd/issues/173

USN-2987-1: GD library vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2987-1
PHP :: Bug #70064 :: imagescale(..., IMG_BICUBIC) leaks memory	Exploit bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=70064
gdImageScaleTwoPass memory leak fix · libgd/libgd@4751b60 · GitHub	Patch github.com text/html	CONFIRM github.com/libgd/libgd/commit/4751b606fa38edc456d627140898a7ec679fcc24
Debian -- Security Information -- DSA-3587-1 libgd2	www.debian.org Depreciated Link text/html	DEBIAN DSA-3587
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
PHP: PHP 5 ChangeLog	www.php.net text/html	CONFIRM www.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	All	All	All	All
Application	Php	Php	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→