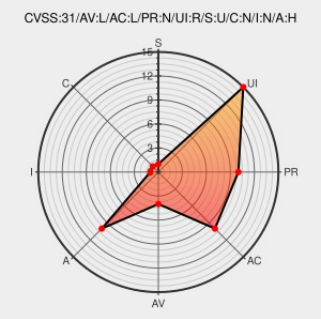
CVE-2015-8900

Published on: 02/27/2017 12:00:00 AM UTC

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

CVE-2015-8900

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



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

The ReadHDRImage function in coders/hdr.c in ImageMagick 6.x and 7.x allows remote attackers to cause a denial of service (infinite loop) via a crafted HDR file.

CVE-2015-8900 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: Requesting CVE for ImageMagick DoS	Mailing List, Patch, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20160606 Re: Requesting CVE for ImageMagic

Fixed infinite loop and added checks for the sscanf result. · ImageMagick/ImageMagick@97aa7d7 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/commit/97aa7d7cfd2027f6ba7ce
Bug 1195260 – CVE-2015-8900 ImageMagick: denial of service flaw in HDR file processing	Issue Tracking Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1195260
oss-security - Re: Requesting CVE for ImageMagick DoS	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20150226 Requesting CVE for ImageMagick Do
Changeset 17845 – ImageMagick	Broken Link web.archive.org text/html Inactive Link Not Archived	CONFIRM trac.imagemagick.org/changeset/17845
Excessive CPU in HDR image - IM6 SVN - convert - 3c1c3e63 - ImageMagick	Exploit Patch Vendor Advisory www.imagemagick.org text/html	CONFIRM www.imagemagick.org/discourse-server/viewtopic.php?f=
Changeset 17846 – ImageMagick	Broken Link web.archive.org text/html Inactive Link Not Archived	CONFIRM trac.imagemagick.org/changeset/17846

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	All	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report