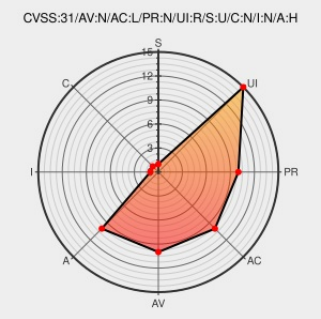
CVE-2015-8903

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

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-8903

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



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

The ReadVICARImage function in coders/vicar.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted VICAR file.

CVE-2015-8903 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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 ImageMagick DoS

oss-security - Re: Requesting CVE for ImageMagick DoS	Exploit Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20150226 Requesting CVE for ImageMagick DoS
Changeset 17856 – ImageMagick	Broken Link web.archive.org text/html Inactive Link Not Archived	CONFIRM trac.imagemagick.org/changeset/17856
Bug 1195271 – CVE-2015-8903 ImageMagick: denial of service flaw in VICAR file processing	Exploit Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1195271
Excessive CPU in VICAR file - IM6 SVN - convert - 783d8806 - ImageMagick	Exploit Vendor Advisory www.imagemagick.org text/html	CONFIRM www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=26933

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→