

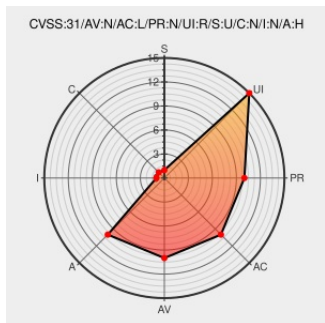


CVE-2015-8902

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

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

CVE-2015-8902

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Imagemagick](#) from [Imagemagick](#) contain the following vulnerability:

The ReadBlobByte function in coders/pdb.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 PDB file.

CVE-2015-8902 has been assigned by [M](#) 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 Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160606 Re: Requesting CVE for ImageMagick DoS

Bug 1195269 – CVE-2015-8902 ImageMagick: denial of service flaw in PDB file processing

Issue Tracking

Third Party Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=1195269

oss-security - Re: Requesting CVE for ImageMagick DoS

Mailing List

Third Party Advisory

www.openwall.com

text/html

MLIST [oss-security] 20150226 Requesting CVE for ImageMagick DoS

Excessive CPU in PDB image - IM6 SVN - convert - c8ad6aba - ImageMagick

Exploit

Vendor Advisory

www.imagemagick.org

text/html

CONFIRM

www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=26932

Changeset 17855 – ImageMagick

Broken Link

web.archive.org

text/html

Inactive Link

Not Archived

CONFIRM

trac.imagemagick.org/changeset/17855

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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