

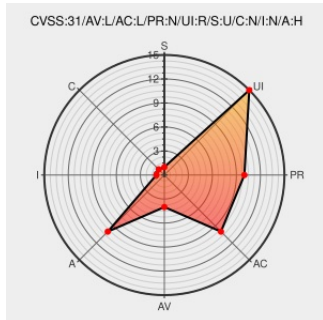


CVE-2015-8900

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 [M](#) [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 DoS
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

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

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)