



CVE-2016-5689

Published on: 12/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5689

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

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

The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of NULL pointer checks.

CVE-2016-5689 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ImageMagick/ChangeLog at 7.0.1-7 · ImageMagick/ImageMagick · GitHub	Release Notes Vendor Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/blob/7.0.1-7/ChangeLog

Add additional checks to DCM reader to prevent data-driven faults (bu... · ImageMagick/ImageMagick@5511ef5 · GitHub	Exploit Vendor Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/commit/5511ef530576ed18fd636
oss-security - Re: Various invalid memory reads in ImageMagick (WPG, DDS, DCM)	Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160617 Re: Various invalid memory reads in I DDS, DCM)
oss-security - Various invalid memory reads in ImageMagick (WPG, DDS, DCM)	Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160614 Various invalid memory reads in Imag DCM)
Various invalid memory accesses in ImageMagick (WPG, DDS, DCM) The Fuzzing Project	Third Party Advisory blog.fuzzing-project.org text/html	MISC blog.fuzzing-project.org/46-Various-invalid-memory-reads-in-Im-DDS,-DCM.html
ImageMagick Multiple Security Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 91283
ImageMagick/ChangeLog at 6.9.4-5 · ImageMagick/ImageMagick · GitHub	Release Notes Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM github.com/ImageMagick/ImageMagick/blob/6.9.4-5/ChangeLog
Oracle Solaris Bulletin - July 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016

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	7.0.1-0	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-1	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-2	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-3	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-4	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-5	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-6	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-0	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-1	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-2	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-3	All	All	All

Application	Imagemagick	Imagemagick	7.0.1-4	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-5	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-6	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
cpe:2.3:a:imagemagick:imagemagick:7.0.1-0:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-1:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-2:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-3:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-4:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-5:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-6:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-0:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-1:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-2:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-3:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-4:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-5:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:7.0.1-6:****:*:*:						
cpe:2.3:a:imagemagick:imagemagick:*:****:*:*:						
cpe:2.3:o:oracle:solaris:11.3:****:*:*:						
cpe:2.3:o:oracle:solaris:11.3:****:*:*:						

No vendor comments have been submitted for this CVE

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](#)