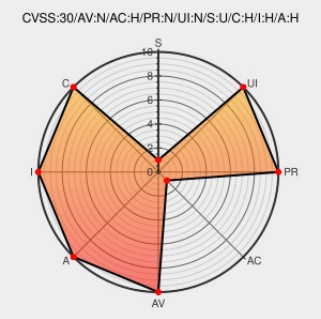
CVE-2016-5688

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

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

CVE-2016-5688

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



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

The WPG parser in ImageMagick before 6.9.4-4 and 7.x before 7.0.1-5, when a memory limit is set, allows remote attackers to have unspecified impact via vectors related to the SetImageExtent return-value check, which trigger (1) a heap-based buffer overflow in the SetPixelIndex function or an invalid write operation in the (2) ScaleCharToQuantum or (3) SetPixelIndex functions.

CVE-2016-5688 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Ensure image extent does not exceed maximum ·	Patch Vendor Advisory	CONFIRM github.com/ImageMagick/ImageMagick/commit/fc43974d34318c834fbf7

ImageMagick/ImageMagick@fc43974 · GitHub	github.com text/html	
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 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
Set pixel cache to undefined if any resource limit is exceeded · ImageMagick/ImageMagick@aecd0ad · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/commit/aecd0ada163a4d6c769c
Commits · ImageMagick/ImageMagick · GitHub	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM github.com/ImageMagick/ImageMagick/commits/6.9.4-4
Commits · ImageMagick/ImageMagick · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/commits/7.0.1-5
Oracle Solaris Bulletin - July 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul201

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	7.0.1-0	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	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:7.0.1-0:*:*:*:*:*:*:*:
- 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:*:*:*:*:*:*:*:*:
- 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

← Previous ID

Next ID→