

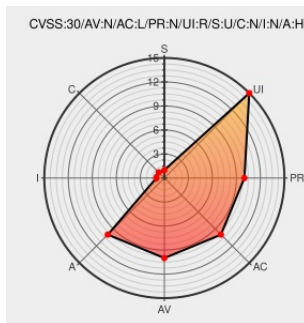


CVE-2018-11251

Published on: 05/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11251

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

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

In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24, there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file.

CVE-2018-11251 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
heap-buffer-overflow in SetGrayscaleImage · Issue #956 · ImageMagick/ImageMagick · GitHub	Exploit Third Party Advisory github.com	CONFIRM github.com/ImageMagick/ImageMagick/issues/956

[text/html](#)

USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices

[Third Party Advisory](#)[usn.ubuntu.com](#)[text/html](#)[UBUNTU USN-3681-1](#)

[SECURITY] [DLA 1394-1] imagemagick security update

[lists.debian.org](#)[text/html](#)

[MLIST \[debian-lts-announce\] 20180626 \[SECURITY\] \[DLA 1394-1\] imagemagick security update](#)

Debian -- Security Information -- DSA-4245-1 imagemagick

[www.debian.org](#)[Deprecated Link](#)[text/html](#)[DEBIAN DSA-4245](#)

[SECURITY] [DLA 1381-1] imagemagick security update

[Third Party Advisory](#)[lists.debian.org](#)[text/html](#)

[MLIST \[debian-lts-announce\] 20180523 \[SECURITY\] \[DLA 1381-1\] imagemagick security update](#)

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	7.0.7-23	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-23	All	All	All

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.7-23:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.7-23:*:*:*:*:

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](#).

