



CVE-2018-11625

Published on: 05/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11625

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

In ImageMagick 7.0.7-37 Q16, SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file.

CVE-2018-11625 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
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
USN-3681-1: ImageMagick vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3681-1
heap-buffer-overflow in MagickCore · Issue #1156 ·	Exploit	MISC

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-37	q16	All	All
Application	Imagemagick	Imagemagick	7.0.7-37	q16	All	All

```
cpe:2.3:o:canonical:ubuntu linux:18.04:*:*:*:its:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:7.0.7-37:q16:***:***:*
```

```
cpe:2.3:a:imagemagick:imagemagick:7.0.7-37:q16:***:***:
```

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