



# CVE-2017-18250

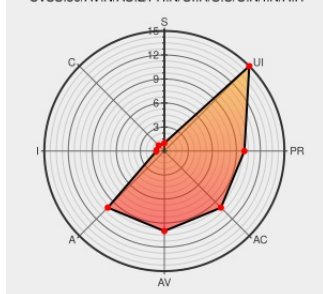
Published on: 03/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

## CVE-2017-18250

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H



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

An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LogOpenCLBuildFailure in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file.

CVE-2017-18250 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                       | Tags                                                                                                               | Link                                                                                     |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| null pointer dereference in LogOpenCLBuildFailure · Issue #793 · ImageMagick/ImageMagick · GitHub | <a href="#">Issue Tracking</a><br><a href="#">Patch</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM</a><br><a href="#">github.com/ImageMagick/ImageMagick/issues/793</a> |

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](mailto: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                                          | <a href="#">Imagemagick</a> | <a href="#">Imagemagick</a> | 7.0.7-0 | All    | All     | All      |
| Application                                          | <a href="#">Imagemagick</a> | <a href="#">Imagemagick</a> | 7.0.7-0 | All    | All     | All      |
| cpe:2.3:a:imagemagick:imagemagick:7.0.7-0:*:*:*:*:*: |                             |                             |         |        |         |          |
| cpe:2.3:a:imagemagick:imagemagick:7.0.7-0:*:*:*:*:*: |                             |                             |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)