



# CVE-2014-9831

Published on: 08/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

## CVE-2014-9831

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

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

coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file.

CVE-2014-9831 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

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

## CVE References

| Description                         | Tags                                                                                                                                                           | Link                                                               |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| oss-security - Re: ImageMagick CVEs | <a href="#">Mailing List</a><br><a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.openwall.com</a><br><a href="#">text/html</a> | <a href="#">MLIST [oss-security] 20160602 Re: ImageMagick CVEs</a> |

404 Not Found

Issue Tracking

Patch

Third Party Advisory

anonscm.debian.org

text/html

Inactive Link

Not Archived

CONFIRM

anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=b68b78e2625122d9f6b6d88ba4df7e85b47b556f

1343487 – (CVE-2014-9831) CVE-2014-9831 ImageMagick: handling of corrupted wpg file

Issue Tracking

Patch

Third Party Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show\_bug.cgi?id=1343487

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> | All     | All    | All     | All      |
| Application | <a href="#">Imagemagick</a> | <a href="#">Imagemagick</a> | All     | All    | All     | All      |

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →