



# CVE-2012-0248

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-0248                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | cert@cert.org                                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2012-06-05 22:55:00 UTC                                                                                                       |
| <b>Updated</b>         | 2020-07-31 18:39:00 UTC                                                                                                       |
| <b>Description</b>     | ImageMagick 6.7.5-7 and earlier allows remote attackers to cause a denial of service (infinite loop and hang) via a crafted i |

## Risk And Classification

### Problem Types: CWE-835

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                      | Product                                  | Version | Update | Edition | Language |
|------------------|-----------------------------|------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 11.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 11.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 11.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 11.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>   | <a href="#">Ubuntu Linux</a>             | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>      | <a href="#">Debian Linux</a>             | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>      | <a href="#">Debian Linux</a>             | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>      | <a href="#">Debian Linux</a>             | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>      | <a href="#">Debian Linux</a>             | 7.0     | All    | All     | All      |
| Application      | <a href="#">Imagemagick</a> | <a href="#">Imagemagick</a>              | All     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>      | <a href="#">Enterprise Linux Desktop</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>      | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>      | <a href="#">Enterprise Linux Desktop</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>      | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |

|                  |                        |                                              |     |     |     |     |
|------------------|------------------------|----------------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Eus</a>         | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Eus</a>         | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 6.2 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Application      | <a href="#">Redhat</a> | <a href="#">Storage</a>                      | 2.0 | All | All | All |
| Application      | <a href="#">Redhat</a> | <a href="#">Storage</a>                      | 2.0 | All | All | All |

| References                                                                                  |  |  |  |               |                                         |  |
|---------------------------------------------------------------------------------------------|--|--|--|---------------|-----------------------------------------|--|
| Reference                                                                                   |  |  |  | Source        | Link                                    |  |
| Red Hat Customer Portal                                                                     |  |  |  | REDHAT        | <a href="#">rhn.redhat.com</a>          |  |
| Security Alerts - Secunia                                                                   |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| About Secunia Research   Flexera                                                            |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| Security Alerts - Secunia                                                                   |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| Security Alerts - Secunia                                                                   |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| 79003                                                                                       |  |  |  | OSVDB         | <a href="#">www.osvdb.org</a>           |  |
| Security Alerts - Secunia                                                                   |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| Security Alerts - Secunia                                                                   |  |  |  | SECUNIA       | <a href="#">secunia.com</a>             |  |
| ImageMagick Buffer Overflow and Denial of Service Vulnerabilities                           |  |  |  | BID           | <a href="#">www.securityfocus.com</a>   |  |
| Debian -- Security Information -- DSA-2427-1 imagemagick                                    |  |  |  | DEBIAN        | <a href="#">www.debian.org</a>          |  |
| Red Hat Customer Portal                                                                     |  |  |  | REDHAT        | <a href="#">rhn.redhat.com</a>          |  |
| Gentoo Linux Documentation -- ImageMagick: User-assisted execution of arbitrary code        |  |  |  | GENTOO        | <a href="#">www.gentoo.org</a>          |  |
| USN-1435-1: ImageMagick vulnerabilities   Ubuntu                                            |  |  |  | UBUNTU        | <a href="#">ubuntu.com</a>              |  |
| ImageMagick • View topic - ImageMagick Invalid Validation and Denial of Service             |  |  |  | CONFIRM       | <a href="#">www.imagemagick.org</a>     |  |
| ImageMagick Bugs Let Remote Users Execute Arbitrary Code and Deny Service - SecurityTracker |  |  |  | SECTrack      | <a href="#">www.securitytracker.com</a> |  |
| CERT-FI - CERT-FI Advisory on issues in ImageMagick                                         |  |  |  | MISC          | <a href="#">www.cert.fi</a>             |  |
| CVE-2015-8126: ImageMagick Denial of Service Vulnerability                                  |  |  |  | CVE-2015-8126 | <a href="#">cve.org</a>                 |  |

|                                                                      |         |                                                |
|----------------------------------------------------------------------|---------|------------------------------------------------|
| CVE Program record                                                   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   |
| NVD vulnerability detail                                             | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> |
| <div><div></div></div>                                               |         |                                                |
| No vendor comments have been submitted for this CVE.                 |         |                                                |
| There are currently no legacy QID mappings associated with this CVE. |         |                                                |

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)