



# CVE-2016-3717

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

## Summary

<b>CVE</b>	CVE-2016-3717
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-05-05 18:59:00 UTC
<b>Updated</b>	2023-02-12 23:20:00 UTC
<b>Description</b>	The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Application	Imagemagick	Imagemagick	7.0.0-0	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-0	All	All	All
Application	Imagemagick	Imagemagick	7.0.0-0	All	All	All
Application	Imagemagick	Imagemagick	7.0.1-0	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node Eus</a>	7.2	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>	7.0	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>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary Eus</a>	6.7z	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary Eus</a>	6.7z	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>	7.0	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>	7.0	All	All	All

## References

Reference	Source	Link	Ta
Debian -- Security Information -- DSA-3580-1 imagemagick	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
[security-announce] openSUSE-SU-2016:1266-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
CVE-2016-3717 - Red Hat Customer Portal	MISC	<a href="http://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	MISC	<a href="http://access.redhat.com">access.redhat.com</a>	
1332505 – (CVE-2016-3717) CVE-2016-3717 ImageMagick: Local file read	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	
[security-announce] openSUSE-SU-2016:1326-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>	Th
oss-security - Re: ImageMagick Is On Fire -- CVE-2016-3714	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Ma
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
USN-2990-1: ImageMagick vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Th
[security-announce] SUSE-SU-2016:1260-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Changelog @ ImageMagick	CONFIRM	<a href="http://www.imagemagick.org">www.imagemagick.org</a>	
CONFIRM	CONFIRM		

Oracle Linux Bulletin - April 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>	
ImageMagick Security Issue - ImageMagick	CONFIRM	<a href="http://www.imagemagick.org">www.imagemagick.org</a>	Ve
[SECURITY] [DLA 1401-1] graphicsmagick security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
ImageMagick: Multiple vulnerabilities (GLSA 201611-21) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
[security-announce] SUSE-SU-2016:1275-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
[security-announce] openSUSE-SU-2016:1261-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
ImageMagick 7.0.1-0 / 6.9.3-9 - 'ImageTragick ' Multiple Vulnerabilities - Multiple dos Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	
ChangeLog · a01518e08c840577cabd7d3ff291a9ba735f7276 · repos / ImageMagick · GitLab	CONFIRM	<a href="http://git.imagemagick.org">git.imagemagick.org</a>	Pa
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	<a href="http://www.slackware.com">www.slackware.com</a>	
Oracle Solaris Bulletin - July 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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

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

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