



# CVE-2014-0190

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

## Summary

<b>CVE</b>	CVE-2014-0190
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-05-08 14:29:00 UTC
<b>Updated</b>	2021-06-16 13:39:00 UTC
<b>Description</b>	The GIF decoder in QtGui in Qt before 5.3 allows remote attackers to cause a denial of service (NULL pointer dereference)

## Risk And Classification

**Problem Types:** CWE-476

## 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>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.04	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.0.0	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.0.1	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.0	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.1	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.2	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.3	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.4	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.1.5	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.2.0	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.2.1	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.2.3	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.3.0	All	All	All
Application	<a href="#">Digia</a>	<a href="#">Qt</a>	4.3.1	All	All	All

Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All
Application	Digia	Qt	4.4.0	All	All	All
Application	Digia	Qt	4.4.1	All	All	All
Application	Digia	Qt	4.4.2	All	All	All
Application	Digia	Qt	4.4.3	All	All	All
Application	Digia	Qt	4.5.0	All	All	All
Application	Digia	Qt	4.5.1	All	All	All
Application	Digia	Qt	4.5.2	All	All	All
Application	Digia	Qt	4.5.3	All	All	All
Application	Digia	Qt	4.6.0	All	All	All
Application	Digia	Qt	4.6.0	rc1	All	All
Application	Digia	Qt	4.6.1	All	All	All
Application	Digia	Qt	4.6.2	All	All	All
Application	Digia	Qt	4.6.3	All	All	All
Application	Digia	Qt	4.6.4	All	All	All
Application	Digia	Qt	4.6.5	All	All	All
Application	Digia	Qt	4.6.5	rc	All	All
Application	Digia	Qt	4.7.0	All	All	All
Application	Digia	Qt	4.7.1	All	All	All
Application	Digia	Qt	4.7.2	All	All	All
Application	Digia	Qt	4.7.3	All	All	All
Application	Digia	Qt	4.7.4	All	All	All
Application	Digia	Qt	4.7.5	All	All	All
Application	Digia	Qt	4.7.6	All	All	All
Application	Digia	Qt	4.7.6	rc	All	All
Application	Digia	Qt	4.8.0	All	All	All
Application	Digia	Qt	4.8.1	All	All	All
Application	Digia	Qt	4.8.2	All	All	All
Application	Digia	Qt	4.8.3	All	All	All
Application	Digia	Qt	4.8.4	All	All	All
Application	Digia	Qt	4.8.5	All	All	All
Application	Digia	Qt	5.0.0	All	All	All

Application	Digia	Qt	5.0.1	All	All	All
Application	Digia	Qt	5.0.2	All	All	All
Application	Digia	Qt	5.1.0	All	All	All
Application	Digia	Qt	5.2.0	All	All	All
Application	Digia	Qt	4.0.0	All	All	All
Application	Digia	Qt	4.0.1	All	All	All
Application	Digia	Qt	4.1.0	All	All	All
Application	Digia	Qt	4.1.1	All	All	All
Application	Digia	Qt	4.1.2	All	All	All
Application	Digia	Qt	4.1.3	All	All	All
Application	Digia	Qt	4.1.4	All	All	All
Application	Digia	Qt	4.1.5	All	All	All
Application	Digia	Qt	4.2.0	All	All	All
Application	Digia	Qt	4.2.1	All	All	All
Application	Digia	Qt	4.2.3	All	All	All
Application	Digia	Qt	4.3.0	All	All	All
Application	Digia	Qt	4.3.1	All	All	All
Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All
Application	Digia	Qt	4.4.0	All	All	All
Application	Digia	Qt	4.4.1	All	All	All
Application	Digia	Qt	4.4.2	All	All	All
Application	Digia	Qt	4.4.3	All	All	All
Application	Digia	Qt	4.5.0	All	All	All
Application	Digia	Qt	4.5.1	All	All	All
Application	Digia	Qt	4.5.2	All	All	All
Application	Digia	Qt	4.5.3	All	All	All
Application	Digia	Qt	4.6.0	All	All	All
Application	Digia	Qt	4.6.0	rc1	All	All
Application	Digia	Qt	4.6.1	All	All	All
Application	Digia	Qt	4.6.2	All	All	All
Application	Digia	Qt	4.6.3	All	All	All
Application	Digia	Qt	4.6.4	All	All	All
Application	Digia	Qt	4.6.5	All	All	All

Application	Digia	Qt	4.6.5	All	All	All
Application	Digia	Qt	4.6.5	rc	All	All
Application	Digia	Qt	4.7.0	All	All	All
Application	Digia	Qt	4.7.1	All	All	All
Application	Digia	Qt	4.7.2	All	All	All
Application	Digia	Qt	4.7.3	All	All	All
Application	Digia	Qt	4.7.4	All	All	All
Application	Digia	Qt	4.7.5	All	All	All
Application	Digia	Qt	4.7.6	All	All	All
Application	Digia	Qt	4.7.6	rc	All	All
Application	Digia	Qt	4.8.0	All	All	All
Application	Digia	Qt	4.8.1	All	All	All
Application	Digia	Qt	4.8.2	All	All	All
Application	Digia	Qt	4.8.3	All	All	All
Application	Digia	Qt	4.8.4	All	All	All
Application	Digia	Qt	4.8.5	All	All	All
Application	Digia	Qt	5.0.0	All	All	All
Application	Digia	Qt	5.0.1	All	All	All
Application	Digia	Qt	5.0.2	All	All	All
Application	Digia	Qt	5.1.0	All	All	All
Application	Digia	Qt	5.2.0	All	All	All
Application	Digia	Qt	All	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Application	Qt	Qt	All	All	All	All

## References

Reference	Source	Link	Tags
openSUSE-SU-2015:0573-1: moderate: Security update for kdebase4-runtime,	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[SECURITY] Fedora 20 Update: qt3-3.3.8b-58.fc20	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 19 Update: qt3-3.3.8b-58.fc19	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
USN-2626-1: Qt vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	
333404 – Crash in QGIFFormat::fillRect while scanning files	CONFIRM	<a href="https://bugs.kde.org">bugs.kde.org</a>	

Qt QtGui GIF Image Handler Local Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
[SECURITY] Fedora 20 Update: qt-4.8.6-2.fc20	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[Announce] Qt Security Advisory: DoS vulnerability in the GIF image handler	MLIST	<a href="http://lists.qt-project.org">lists.qt-project.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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

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