



# CVE-2013-7447

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

## Summary

<b>CVE</b>	CVE-2013-7447
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-17 15:59:00 UTC
<b>Updated</b>	2016-12-03 03:00:00 UTC
<b>Description</b>	Integer overflow in the gdk_cairo_set_source_pixbuf function in gdk/gdkcairo.c in GTK+ before 3.9.8, as used in eom, gnom

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## 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>	15.10	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>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Application	<a href="#">Gtk</a>	<a href="#">Gtk</a>	All	All	All	All
Application	<a href="#">Gtk</a>	<a href="#">Gtk</a>	All	All	All	All
Operating System	<a href="#">Samsung</a>	<a href="#">X14j Firmware</a>	t-ms14jakucb-1102.5	All	All	All

## References

Reference	Source	Link
openSUSE-SU-2016:0647-1: moderate: Security update for eog	SUSE	<a href="#">lists.opensuse.org</a>
USN-2898-1: GTK+ vulnerability   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>
EOM crashes when trying to open a large PNG file · Issue #93 · mate-desktop/eom · GitHub	CONFIRM	<a href="#">github.com</a>
Avoid integer overflow (894b1ae7) · Commits · GNOME / gtk · GitHub	CONFIRM	<a href="#">git.gnome.org</a>
oss-security - CVE Request: eom, gnome-photos, eog, gambas3, thunar, pinpoint, gtk+2.0	MLIST	<a href="#">www.openwall.com</a>

GTK+ CVE-2013-7447 Integer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
oss-security - Re: CVE Request: eom, gnome-photos, eog, gambas3, thunar, pinpoint, gtk+2.0	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Bug #1540811 "[GDK] patch - avoid integer overflow when allocati...": Bugs : gtk+2.0 package : Ubuntu	CONFIRM	<a href="http://bugs.launchpad.net">bugs.launchpad.net</a>
USN-2898-2: Eye of GNOME vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
Bug 703220 – Memory allocation integer overflow in gdk_cairo_set_source_pixbuf on large pixbufs	CONFIRM	<a href="http://bugzilla.gnome.org">bugzilla.gnome.org</a>
gtk+ - Multi-platform toolkit	CONFIRM	<a href="http://git.gnome.org">git.gnome.org</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>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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)