



# CVE-2013-6425

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

## Summary

<b>CVE</b>	CVE-2013-6425
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-01-18 19:55:00 UTC
<b>Updated</b>	2023-02-13 00:29:00 UTC
<b>Description</b>	Integer underflow in the pixman_trapezoid_valid macro in pixman.h in Pixman before 0.32.0, as used in X.Org server and c

## Risk And Classification

### Problem Types: CWE-191

## 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>	12.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.10	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>	12.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	13.10	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
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Application	<a href="#">Pixman</a>	<a href="#">Pixman</a>	All	All	All	All
Application	<a href="#">Pixman</a>	<a href="#">Pixman</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>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	6.5	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>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	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

## References

Reference	Source	Li
67484 – Corrupted CustomShape crashes Xorg	MISC	bu
oss-security - CVE Request: xorg-server and pixman	MLIST	w
oss-security - Re: CVE Request: xorg-server and pixman	MLIST	w
openSUSE-SU-2014:0007-1: moderate: update for pixman	SUSE	lis
CVE-2013-6425 - Red Hat Customer Portal	MISC	ac
Bug #1197921 "LibreOffice spreadsheet causes full Xorg crash wit..." : Bugs : "xorg-server" package : Ubuntu	MISC	bu
openSUSE-SU-2014:0145-1: moderate: update for pixman	SUSE	lis
1037975 – (CVE-2013-6425) CVE-2013-6425 pixman: integer underflow when handling trapezoids	MISC	bu
openSUSE-SU-2014:0011-1: moderate: update for pixman	SUSE	lis
Red Hat Customer Portal	REDHAT	

Red Hat Customer Portal	REDHAT	rr
openSUSE-SU-2014:0014-1: moderate: update for pixman	SUSE	lis
[Pixman] [ANNOUNCE] pixman release 0.32.0 now available	MLIST	lis
USN-2047-1: pixman vulnerability   Ubuntu	UBUNTU	w
Debian -- Security Information -- DSA-2823-1 pixman	DEBIAN	w
pixman - Pixman: The pixel-manipulation library for X and cairo. (mirrored from <a href="https://gitlab.freedesktop.org/pixman/pixman">https://gitlab.freedesktop.org/pixman/pixman</a> )	CONFIRM	c
Red Hat Customer Portal	MISC	ac
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)