



CVE-2013-6424

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2013-6424 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2014-01-18 19:55:00 UTC |
| Updated | 2023-02-13 04:49:00 UTC |
| Description | Integer underflow in the xTrapezoidValid macro in render/picture.h in X.Org allows context-dependent attackers to cause a |

Risk And Classification

Problem Types: CWE-191

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 | 14.10 | All | All | All |
| Operating System | Debian | Debian Linux | 6.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Opensuse | Opensuse | 12.2 | All | All | All |
| Operating System | Opensuse | Opensuse | 12.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Application | Pixman | Pixman | All | All | All | All |
| Application | X.org | X Server | - | All | All | All |
| Application | X.org | X Server | - | All | All | All |

References

| Reference | Source | Link |
|---|---------|--------------------------------------|
| 67484 – Corrupted CustomShape crashes Xorg | CONFIRM | bugs.freedesktop.org |
| X.Org X Server: Multiple vulnerabilities (GLSA 201701-64) — Gentoo Security | GENTOO | security.gentoo.org |
| [PATCH] exa: only draw valid trapezoids | MLIST | lists.x.org |

| | | |
|--|---------|--|
| oss-security - CVE Request: xorg-server and pixman | MLIST | www.openwall.c |
| oss-security - Re: CVE Request: xorg-server and pixman | MLIST | www.openwall.c |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com |
| Debian -- Security Information -- DSA-2822-1 xorg-server | DEBIAN | www.debian.org |
| Bug #1197921 "LibreOffice spreadsheet causes full Xorg crash wit..." : Bugs : "xorg-server" package : Ubuntu | CONFIRM | bugs.launchpad. |
| USN-2500-1: X.Org X server vulnerabilities Ubuntu | UBUNTU | www.ubuntu.com |
| openSUSE-SU-2013:1965-1: moderate: xorg-x11-server: fixed an overflow in | SUSE | lists.opensuse.o |
| Red Hat Customer Portal | MISC | access.redhat.co |
| X.Org Server: Multiple vulnerabilities (GLSA 201710-30) — Gentoo Security | GENTOO | security.gentoo.c |
| access.redhat.com CVE-2013-6424 | MISC | access.redhat.co |
| 1037984 – (CVE-2013-6424) CVE-2013-6424 xorg-x11-server: integer underflow when handling trapezoids | MISC | bugzilla.redhat.c |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710555](#) Gentoo Linux X.Org X Server Multiple Vulnerabilities (GLSA 201701-64)

[710562](#) Gentoo Linux X.Org Server Multiple Vulnerabilities (GLSA 201710-30)

© [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](#)