



CVE-2007-4730

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

Summary

CVE	CVE-2007-4730
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-11 19:17:00 UTC
Updated	2017-09-29 01:29:00 UTC
Description	Buffer overflow in the compNewPixmap function in compalloc.c in the Composite extension for the X.org X11 server before

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	X.org	Xorg-server	1.01	All	All	All
Application	X.org	Xorg-server	1.02	All	All	All
Application	X.org	Xorg-server	1.1	All	All	All
Application	X.org	Xorg-server	1.2	All	All	All
Application	X.org	Xorg-server	1.3	All	All	All
Application	X.org	Xorg-server	1.01	All	All	All
Application	X.org	Xorg-server	1.02	All	All	All
Application	X.org	Xorg-server	1.1	All	All	All
Application	X.org	Xorg-server	1.2	All	All	All
Application	X.org	Xorg-server	1.3	All	All	All

References

Reference	Source	Link
Debian update for xorg-server - Advisories - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xfc
Advisories Mandriva	MANDRIVA	www.mandriva
X.Org X Server Composite Extension Local Buffer Overflow Vulnerability	BID	www.security

Debian -- Security Information -- DSA-1372-1 xorg-server	DEBIAN	www.debian.org
Webmail - OVH	VUPEN	www.vupen.com
SUSE update for XOrg - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
X.org X11 Composite Pixmap Privilege Escalation Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Avaya Products X.org X11 Composite Pixmap Privilege Escalation - Advisories - Secunia	SECUNIA	secunia.com
Advisories Mandriva	MANDRIVA	www.mandriva.com
issues.rpath.com/browse/RPL-1728	CONFIRM	issues.rpath.com
X.Org X server: Composite local privilege escalation — Gentoo Linux Documentation	GENTOO	security.gentoo.org
Red Hat update for xorg-x11 - Advisories - Secunia	SECUNIA	secunia.com
USN-514-1: X.org vulnerability Ubuntu	UBUNTU	www.ubuntu.com
Mandriva update for x11-server - Advisories - Secunia	SECUNIA	secunia.com
37726	OSVDB	osvdb.org
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	www.gentoo.org
wiki.rpath.com/wiki/Advisories:rPSA-2007-0187	CONFIRM	wiki.rpath.com
Gentoo update for xorg-server - Advisories - Secunia	SECUNIA	secunia.com
X Server Bug in compNewPixmap() Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack	www.securitytracker.com
Support	REDHAT	www.redhat.com
rPath update for xorg-x11 - Advisories - Secunia	SECUNIA	secunia.com
Security Announcement	SUSE	www.novell.com
Ubuntu update for xorg-server - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Bug 191964 - x11-base/xorg-server < 1.3.0.0-r1 Composite local privilege escalation (CVE-2007-4730)	CONFIRM	bugs.gentoo.org
7447 – X crashes when 32-bit windows are resized on a 16-bit desktop	CONFIRM	bugs.freedesktop.org
Gentoo Itsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
[ANNOUNCE] xorg-server 1.4	MLIST	lists.freedesktop.org
ASA-2007-394 (RHSA-2007-0898)	CONFIRM	support.avaya.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-09-26	Joshua Bressers	This flaw was fixed for Red Hat Enterprise Linux 4 in RHSA-2007-0898: https://rhn.redhat.com

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](#).

Free CVE JSON API [cve.report/api](#)

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