



# CVE-2023-6377

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

## Summary

<b>CVE</b>	CVE-2023-6377
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-12-13 07:15:00 UTC
<b>Updated</b>	2024-01-31 13:15:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.2	All	All	All
Application	<a href="#">Tigervnc</a>	<a href="#">Tigervnc</a>	-	All	All	All
Application	<a href="#">X.org</a>	<a href="#">Xwayland</a>	All	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X Server</a>	All	All	All	All

## References

Reference	Source	Link
RHSA-2024:0020		<a href="#">access.redh</a>
RHSA-2024:0014		<a href="#">access.redh</a>
RHSA-2024:0016		<a href="#">access.redh</a>
RHSA-2024:0010		<a href="#">access.redh</a>

RHSA-2024:0010	access.redh	
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	lists.fedora	
gitlab.freedesktop.org/xorg/xserver/-/commit/0c1a93d319558fe3ab2d94f51d174b4f93810afd	gitlab.freed	
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	lists.fedora	
lists.debian.org/debian-lts-announce/2023/12/msg00013.html	lists.debian	
RHSA-2023:7886	access.redh	
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	lists.fedora	
[SECURITY] Fedora 38 Update: tigervnc-1.13.1-9.fc38 - package-announce - Fedora Mailing-Lists	lists.fedora	
RHSA-2024:0015	access.redh	
www.debian.org/security/2023/dsa-5576	www.debian	
RHSA-2024:0006	access.redh	
RHSA-2024:0017	access.redh	
lists.x.org/archives/xorg-announce/2023-December/003435.html	lists.x.org	
X.Org X Server, XWayland: Multiple Vulnerabilities (GLSA 202401-30) — Gentoo security	security.ger	
December 2023 X.Org X Server Vulnerabilities in NetApp Products   NetApp Product Security	security.net	
oss-security - FW: X.Org Security Advisory: Issues in X.Org X server prior to 21.1.10 and Xwayland prior to 23.2.3	www.openv	
lists.debian.org/debian-lts-announce/2023/12/msg00008.html	lists.debian	
RHBZ#2253291	bugzilla.red	
access.redhat.com/security/cve/CVE-2023-6377	access.redh	
RHSA-2024:0018	access.redh	
RHSA-2024:0009	access.redh	
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- 161260 Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2024-0009)
- 161261 Oracle Enterprise Linux Security Update for tigervnc (ELSA-2024-0006)
- 161265 Oracle Enterprise Linux Security Update for tigervnc (ELSA-2024-0010)
- 161267 Oracle Enterprise Linux Security Update for tigervnc (ELSA-2024-0018)
- 200008 Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-6555-2)
- 200009 Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-6555-1)
- 242635 Red Hat Update for tigervnc (RHSA-2023:7886)

<a href="#">242638</a> Red Hat Update for tigervnc (RHSA-2024:0017)
<a href="#">242648</a> Red Hat Update for tigervnc (RHSA-2024:0006)
<a href="#">242649</a> Red Hat Update for tigervnc (RHSA-2024:0020)
<a href="#">242650</a> Red Hat Update for tigervnc (RHSA-2024:0015)
<a href="#">242652</a> Red Hat Update for tigervnc (RHSA-2024:0014)
<a href="#">242654</a> Red Hat Update for tigervnc (RHSA-2024:0018)
<a href="#">242660</a> Red Hat Update for tigervnc (RHSA-2024:0010)
<a href="#">242662</a> Red Hat Update for tigervnc (RHSA-2024:0016)
<a href="#">242665</a> Red Hat Update for xorg-x11-server (RHSA-2024:0009)
<a href="#">257273</a> Centos Security Update for tigervnc
<a href="#">257274</a> Centos Security Update for xorg-x11-server
<a href="#">257276</a> CentOS Security Update for tigervnc (CESA-2024:0006)
<a href="#">257278</a> CentOS Security Update for xorg-x11-server (CESA-2024:0009)
<a href="#">284828</a> Fedora Security Update for xorg (FEDORA-2023-77c8903bcb)
<a href="#">284852</a> Fedora Security Update for tigervnc (FEDORA-2023-ec02e360af)
<a href="#">285097</a> Fedora Security Update for xorg (FEDORA-2023-93940b58fd)
<a href="#">285098</a> Fedora Security Update for tigervnc (FEDORA-2023-52460bedda)
<a href="#">296108</a> Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
<a href="#">357185</a> Amazon Linux Security Advisory for xorg-x11-server : AL2012-2024-484
<a href="#">357249</a> Amazon Linux Security Advisory for xorg-x11-server : ALAS2023-2024-522
<a href="#">379273</a> Alibaba Cloud Linux Security Update for xorg-x11-server (ALINUX2-SA-2024:0002)
<a href="#">379625</a> Alibaba Cloud Linux Security Update for tigervnc (ALINUX3-SA-2024:0028)
<a href="#">505836</a> Alpine Linux Security Update for xorg-server
<a href="#">6000380</a> Debian Security Update for xorg-server (DLA 3686-1)
<a href="#">6000381</a> Debian Security Update for xorg-server (DSA 5576-1)
<a href="#">6000388</a> Debian Security Update for xorg-server (DLA 3686-2)
<a href="#">6000389</a> Debian Security Update for xorg-server (DSA 5576-2)
<a href="#">673396</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1210)
<a href="#">673399</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1352)

673339 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1302)
673442 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1307)
673626 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1232)
673924 EulerOS Security Update for tigervnc (EulerOS-SA-2024-1304)
673929 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1254)
673935 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1330)
674012 EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1190)
691374 Free Berkeley Software Distribution (FreeBSD) Security Update for xorg (972568d6-3485-40ab-80ff-994a8aaf9683)
710847 Gentoo Linux X.Org X Server, XWayland Multiple Vulnerabilities (GLSA 202401-30)
755500 SUSE Enterprise Linux Security Update for xwayland (SUSE-SU-2023:4926-1)
755501 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4925-1)
755514 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4935-1)
755515 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4934-1)
755528 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4949-1)
941513 AlmaLinux Security Update for tigervnc (ALSA-2024:0010)
941516 AlmaLinux Security Update for tigervnc (ALSA-2024:0018)

© [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](#)