



# CVE-2023-5380

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

## Summary

<b>CVE</b>	CVE-2023-5380
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-25 20:15:00 UTC
<b>Updated</b>	2024-01-31 13:15:00 UTC
<b>Description</b>	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configura

## Risk And Classification

**Problem Types:** CWE-416

## 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>	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="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	39	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
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
[SECURITY] Fedora 38 Update: xorg-x11-server-1.20.14-26.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraprojec</a>
[SECURITY] Fedora 38 Update: tigervnc-1.13.1-6.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraprojec</a>
2244736 – (CVE-2023-5380) CVE-2023-5380 xorg-x11-server: Use-after-free bug in DestroyWindow	MISC	<a href="#">bugzilla.redhat.cc</a>
[SECURITY] Fedora 39 Update: xorg-x11-server-1.20.14-26.fc39 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraprojec</a>

lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		lists.fedoraprojec
Debian -- Security Information -- DSA-5534-1 xorg-server	MISC	www.debian.org
cve-details	MISC	access.redhat.co
RHSA-2023:7428		access.redhat.co
[SECURITY] Fedora 37 Update: xorg-x11-server-1.20.14-26.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraprojec
X.Org X Server, XWayland: Multiple Vulnerabilities (GLSA 202401-30) — Gentoo security		security.gentoo.o
security.netapp.com/advisory/ntap-20231130-0004		security.netapp.c
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		lists.fedoraprojec
X.Org Security Advisory: Issues in X.Org X server prior to 21.1.9 and Xwayland prior to 23.2.2	MISC	lists.x.org
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

161193 Oracle Enterprise Linux Security Update for tigervnc (ELSA-2023-7428)
199866 Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-6453-1)
199877 Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-6453-2)
242499 Red Hat Update for tigervnc (RHSA-2023:7428)
284686 Fedora Security Update for xorg (FEDORA-2023-1f4f1b8365)
284725 Fedora Security Update for xorg (FEDORA-2023-f111d2f306)
284729 Fedora Security Update for tigervnc (FEDORA-2023-dbacf5d9f6)
284745 Fedora Security Update for tigervnc (FEDORA-2023-4708733ccc)
285157 Fedora Security Update for tigervnc (FEDORA-2023-4bb75fa8f2)
285174 Fedora Security Update for xorg (FEDORA-2023-b88929bc79)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
356618 Amazon Linux Security Advisory for xorg-x11-server : ALAS2023-2023-404
356738 Amazon Linux Security Advisory for xorg-x11-server : ALAS2-2023-2335
356746 Amazon Linux Security Advisory for xorg-x11-server : ALAS-2023-1884
356991 Amazon Linux Security Advisory for xorg-x11-server : AL2012-2023-475
379276 Alibaba Cloud Linux Security Update for tigervnc (ALINUX2-SA-2023:0050)

<a href="#">503445</a> Alpine Linux Security Update for xorg-server
<a href="#">506278</a> Alpine Linux Security Update for xorg-server
<a href="#">6000255</a> Debian Security Update for xorg-server (DLA 3631-1)
<a href="#">6000298</a> Debian Security Update for xorg-server (DSA 5534-1)
<a href="#">673442</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1307)
<a href="#">673495</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1169)
<a href="#">673515</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1131)
<a href="#">673733</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1115)
<a href="#">691339</a> Free Berkeley Software Distribution (FreeBSD) Security Update for xorg (9e2fdcf7-e237-4393-9fa5-2d50908c66b3)
<a href="#">710847</a> Gentoo Linux X.Org X Server, XWayland Multiple Vulnerabilities (GLSA 202401-30)
<a href="#">755188</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4272-1)
<a href="#">755191</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4269-1)
<a href="#">755204</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4292-1)
<a href="#">755217</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:4338-1)

© [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](#)**