



# CVE-2023-0494

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-0494
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-27 21:15:00 UTC
<b>Updated</b>	2023-05-30 06:16:00 UTC
<b>Description</b>	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited.

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Fedoraproject	Fedora	36	All
Operating System	Fedoraproject	Fedora	37	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	8.1	All
Operating System	Redhat	Enterprise Linux	9.0	All
Operating System	Redhat	Enterprise Linux Aus	8.4	All
Operating System	Redhat	Enterprise Linux Aus	8.6	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux Eus	9.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	7.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	8.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Scientific Computing</a>	7.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.1	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Update Services For Sap Solutions</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Workstation</a>	7.0	All
Application	<a href="#">X.org</a>	<a href="#">X Server</a>	All	All

## References

Reference	Source
<a href="#">Xi: fix potential use-after-free in DeepCopyPointerClasses (0ba6d8c3) · Commits · xorg / xserver · GitLab</a>	MISC
<a href="#">X.Org X server, XWayland: Multiple Vulnerabilities (GLSA 202305-30) — Gentoo security</a>	GENTO
<a href="#">X.Org Security Advisory: Security issue in the X server</a>	MISC
<a href="#">2165995 – (CVE-2023-0494) CVE-2023-0494 xorg-x11-server: DeepCopyPointerClasses use-after-free leads to privilege elevation</a>	MISC
<a href="#">CVE Program record</a>	CVE.OF
<a href="#">NVD vulnerability detail</a>	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">160451</a> Oracle Enterprise Linux Security Update for tigervnc (ELSA-2023-0622)
<a href="#">160452</a> Oracle Enterprise Linux Security Update for tigervnc (ELSA-2023-0662)
<a href="#">160455</a> Oracle Enterprise Linux Security Update for tigervnc and xorg-x11-server (ELSA-2023-0675)

<a href="#">160631</a> Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2023-2248)
<a href="#">160633</a> Oracle Enterprise Linux Security Update for xorg-x11-server-xwayland (ELSA-2023-2249)
<a href="#">160677</a> Oracle Enterprise Linux Security Update for xorg-x11-server-xwayland (ELSA-2023-2805)
<a href="#">160679</a> Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2023-2806)
<a href="#">181545</a> Debian Security Update for xorg-server (DSA 5342-1)
<a href="#">181564</a> Debian Security Update for xorg-server (DLA 3310-1)
<a href="#">183751</a> Debian Security Update for xwaylandxorg-server (CVE-2023-0494)
<a href="#">199149</a> Ubuntu Security Notification for X.Org X Server Vulnerability (USN-5846-1)
<a href="#">199494</a> Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-5778-2)
<a href="#">241169</a> Red Hat Update for tigervnc (RHSA-2023:0623)
<a href="#">241176</a> Red Hat Update for tigervnc (RHSA-2023:0622)
<a href="#">241177</a> Red Hat Update for tigervnc (RHSA-2023:0663)
<a href="#">241178</a> Red Hat Update for tigervnc (RHSA-2023:0662)
<a href="#">241179</a> Red Hat Update for tigervnc (RHSA-2023:0664)
<a href="#">241182</a> Red Hat Update for tigervnc and xorg-x11-server (RHSA-2023:0675)
<a href="#">241415</a> Red Hat Update for xorg-x11-server (RHSA-2023:2248)
<a href="#">241448</a> Red Hat Update for xorg-x11-server-xwayland (RHSA-2023:2249)
<a href="#">241510</a> Red Hat Update for xorg-x11-server (RHSA-2023:2806)
<a href="#">241537</a> Red Hat Update for xorg-x11-server-xwayland (RHSA-2023:2805)
<a href="#">241624</a> Red Hat Update for tigervnc (RHSA-2023:0671)
<a href="#">241660</a> Red Hat Update for tigervnc (RHSA-2023:0665)
<a href="#">257221</a> CentOS Security Update for tigervnc (CESA-2023:0675)
<a href="#">283699</a> Fedora Security Update for xorg (FEDORA-2023-83b2d37c6a)
<a href="#">283703</a> Fedora Security Update for tigervnc (FEDORA-2023-4d443bd03f)
<a href="#">283704</a> Fedora Security Update for xorg (FEDORA-2023-d33a0f8471)
<a href="#">283737</a> Fedora Security Update for xorg (FEDORA-2023-fb5022e741)
<a href="#">283738</a> Fedora Security Update for xorg (FEDORA-2023-1ebf4507df)
<a href="#">284279</a> Fedora Security Update for tigervnc (FEDORA-2023-c41e8f24bb)
<a href="#">296099</a> Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)

<a href="#">354800</a> Amazon Linux Security Advisory for xorg-x11-server : ALAS2-2023-1982
<a href="#">354840</a> Amazon Linux Security Advisory for xorg-x11-server : ALAS-2023-1702
<a href="#">355067</a> Amazon Linux Security Advisory for xorg-x11-server : AL2012-2023-391
<a href="#">355107</a> Amazon Linux Security Advisory for tigervnc : ALAS-2023-1746
<a href="#">355245</a> Amazon Linux Security Advisory for xorg-x11-server : ALAS2023-2023-131
<a href="#">377994</a> Alibaba Cloud Linux Security Update for tigervnc and xorg-x11-server (ALINUX2-SA-2023:0010)
<a href="#">377998</a> Alibaba Cloud Linux Security Update for tigervnc (ALINUX3-SA-2023:0022)
<a href="#">378649</a> Alibaba Cloud Linux Security Update for xorg-x11-server (ALINUX3-SA-2023:0062)
<a href="#">379627</a> Alibaba Cloud Linux Security Update for xorg-x11-server-xwayland (ALINUX3-SA-2024:0044)
<a href="#">502972</a> Alpine Linux Security Update for xorg-server
<a href="#">502975</a> Alpine Linux Security Update for xwayland
<a href="#">505839</a> Alpine Linux Security Update for xorg-server
<a href="#">505842</a> Alpine Linux Security Update for xwayland
<a href="#">673016</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2023-1989)
<a href="#">673026</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2023-1967)
<a href="#">673075</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2023-2180)
<a href="#">673084</a> EulerOS Security Update for tigervnc (EulerOS-SA-2023-2176)
<a href="#">673158</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2023-2281)
<a href="#">673161</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2023-2305)
<a href="#">673396</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1210)
<a href="#">673442</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1307)
<a href="#">673924</a> EulerOS Security Update for tigervnc (EulerOS-SA-2024-1304)
<a href="#">674012</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2024-1190)
<a href="#">691052</a> Free Berkeley Software Distribution (FreeBSD) Security Update for xorg (6cc63bf5-a727-4155-8ec4-68b626475e68)
<a href="#">710738</a> Gentoo Linux X.Org X server, XWayland Multiple Vulnerabilities (GLSA 202305-30)
<a href="#">753627</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:0282-1)
<a href="#">753643</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:0288-1)
<a href="#">753644</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:0287-1)

753645 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:0286-1)
753648 SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2023:0285-1)
940919 AlmaLinux Security Update for tigervnc (ALSA-2023:0662)
940921 AlmaLinux Security Update for tigervnc (ALSA-2023:0622)
941042 AlmaLinux Security Update for xorg-x11-server (ALSA-2023:2248)
941062 AlmaLinux Security Update for xorg-x11-server-Xwayland (ALSA-2023:2249)
941068 AlmaLinux Security Update for xorg-x11-server (ALSA-2023:2806)
941119 AlmaLinux Security Update for xorg-x11-server-Xwayland (ALSA-2023:2805)
960530 Rocky Linux Security Update for tigervnc (RLSA-2023:0622)
960558 Rocky Linux Security Update for tigervnc (RLSA-2023:0662)

© [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](#)