



# CVE-2022-2319

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

## Summary

<b>CVE</b>	CVE-2022-2319
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-01 21:15:00 UTC
<b>Updated</b>	2023-02-12 22:15:00 UTC
<b>Description</b>	A flaw was found in the Xorg-x11-server. An out-of-bounds access issue can occur in the ProcXkbSetGeometry function du

## Risk And Classification

**Problem Types:** CWE-1320

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	X.org	Xorg-server	21.1.0	All	All	All

## References

### Reference

- Red Hat Customer Portal - Access to 24x7 support and knowledge
- [server 21.1] Fix CVE-2022-2319, CVE-2022-2320 (1939) · Merge requests · xorg / xserver · GitLab
- Red Hat Customer Portal - Access to 24x7 support and knowledge
- September 2022 X.Org X Server Vulnerabilities in NetApp Products | NetApp Product Security
- ZDI-22-964 | Zero Day Initiative
- X.Org Security Advisory: July 12, 2022
- Red Hat Customer Portal - Access to 24x7 support and knowledge
- Red Hat Customer Portal - Access to 24x7 support and knowledge
- Red Hat Customer Portal - Access to 24x7 support and knowledge
- X.Org X server, XWayland: Multiple Vulnerabilities (GLSA 202210-30) — Gentoo security
- Fix CVE-2022-2319, CVE-2022-2320 (1938) · Merge requests · xorg / xserver · GitLab
- 2106671 – (CVE-2022-2319, ZDI-CAN-16062) CVE-2022-2319 xorg-x11-server: X.Org Server ProcXkbSetGeometry out-of-bounds access
- CVE Program record

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160023](#) Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2022-5905)

[160220](#) Oracle Enterprise Linux Security Update for xorg-x11-server and xorg-x11-server-xwayland (ELSA-2022-7583)

[160269](#) Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2022-8221)

[160298](#) Oracle Enterprise Linux Security Update for xorg-x11-server-xwayland (ELSA-2022-8222)

[180917](#) Debian Security Update for xorg-server (DLA 3068-1)

[180918](#) Debian Security Update for xorg-server (DSA 5199-1)

[183941](#) Debian Security Update for xwaylandxorg-server (CVE-2022-2319)

[198854](#) Ubuntu Security Notification for X.Org X Server Vulnerabilities (USN-5510-1)

[240593](#) Red Hat Update for xorg-x11-server (RHSA-2022:5905)

[240841](#) Red Hat Update for xorg-x11-server and xorg-x11-server-xwayland (RHSA-2022:7583)

[240872](#) Red Hat Update for xorg-x11-server (RHSA-2022:8221)

[240883](#) Red Hat Update for xorg-x11-server-xwayland (RHSA-2022:8222)

[257186](#) CentOS Security Update for xorg-x11-server (CESA-2022:5905)

[282936](#) Fedora Security Update for xorg (FEDORA-2022-856bb475b7)

[282937](#) Fedora Security Update for xorg (FEDORA-2022-6807c29d58)

[282983](#) Fedora Security Update for xorg (FEDORA-2022-8e787b2a5c)

[282984](#) Fedora Security Update for xorg (FEDORA-2022-573714ca6b)

[296083](#) Oracle Solaris 11.4 Support Repository Update (SRU) 49.126.2 Missing (CPUOCT2022)

[354077](#) Amazon Linux Security Advisory for xorg-x11-server : ALAS2-2022-1856

[502430](#) Alpine Linux Security Update for xorg-server

[502970](#) Alpine Linux Security Update for xorg-server

[505837](#) Alpine Linux Security Update for xorg-server

[672143](#) EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2452)

[672206](#) EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2484)

[672207](#) EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2485)

<a href="#">672227</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2640)
<a href="#">672267</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2672)
<a href="#">672279</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2704)
<a href="#">672334</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2785)
<a href="#">672385</a> EulerOS Security Update for xorg-x11-server (EulerOS-SA-2022-2750)
<a href="#">710658</a> Gentoo Linux X.Org X server, XWayland Multiple Vulnerabilities (GLSA 202210-30)
<a href="#">752337</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2375-1)
<a href="#">752339</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2369-1)
<a href="#">752343</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2373-1)
<a href="#">752344</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2374-1)
<a href="#">752345</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2370-1)
<a href="#">752346</a> SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2022:2371-1)
<a href="#">940755</a> AlmaLinux Security Update for xorg-x11-server and xorg-x11-server-Xwayland (ALSA-2022:7583)
<a href="#">940806</a> AlmaLinux Security Update for xorg-x11-server-Xwayland (ALSA-2022:8222)
<a href="#">940807</a> AlmaLinux Security Update for xorg-x11-server (ALSA-2022:8221)
<a href="#">960185</a> Rocky Linux Security Update for xorg-x11-server and xorg-x11-server-Xwayland (RLSA-2022:7583)
<a href="#">960508</a> Rocky Linux Security Update for xorg-x11-server-Xwayland (RLSA-2022:8222)
<a href="#">960627</a> Rocky Linux Security Update for xorg-x11-server (RLSA-2022:8221)

© [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](#)**