



Red Hat Product Errata    RHSA-2024:2995 - Security Advisory

# RHSA-2024:2995 - Security Advisory

Issued: 2024-05-22    Updated: 2024-05-22

[Overview](#)

[Updated Packages](#)

## Synopsis

Moderate: xorg-x11-server security update

## Type/Severity

Security Advisory: Moderate

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for xorg-x11-server is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## Description

X.Org is an open-source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Security Fix(es):

- xorg-x11-server: Out-of-bounds write in XIChangeDeviceProperty/RRChangeOutputProperty (CVE-2023-5367)
- xorg-x11-server: out-of-bounds memory reads/writes in XKB button actions (CVE-2023-6377)
- xorg-x11-server: out-of-bounds memory read in RRChangeOutputProperty and RRChangeProviderProperty (CVE-2023-6478)
- xorg-x11-server: reattaching to different master device may lead to out-of-bounds memory access (CVE-2024-0229)
- xorg-x11-server: SELinux unlabeled GLX PBuffer (CVE-2024-0408)
- xorg-x11-server: SELinux context corruption (CVE-2024-0409)
- xorg-x11-server: heap buffer overflow in XISendDeviceHierarchyEvent (CVE-2024-21885)
- xorg-x11-server: heap buffer overflow in DisableDevice (CVE-2024-21886)
- xorg-x11-server: Use-after-free bug in DestroyWindow (CVE-2023-5380)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.10 Release Notes linked from the References section.

## Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 

## Affected Products

- Red Hat Enterprise Linux for x86\_64 8 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for x86\_64 8 x86\_64
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64

- Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 8.10 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

## Fixes

- [BZ - 2243091](#) - CVE-2023-5367 xorg-x11-server: Out-of-bounds write in XIChangeDeviceProperty/RRChangeOutputProperty
- [BZ - 2244736](#) - CVE-2023-5380 xorg-x11-server: Use-after-free bug in DestroyWindow
- [BZ - 2253291](#) - CVE-2023-6377 xorg-x11-server: out-of-bounds memory reads/writes in XKB button actions
- [BZ - 2253298](#) - CVE-2023-6478 xorg-x11-server: out-of-bounds memory read in RRChangeOutputProperty and RRChangeProviderProperty
- [BZ - 2256540](#) - CVE-2024-21885 xorg-x11-server: heap buffer overflow in XISendDeviceHierarchyEvent
- [BZ - 2256542](#) - CVE-2024-21886 xorg-x11-server: heap buffer overflow in DisableDevice
- [BZ - 2256690](#) - CVE-2024-0229 xorg-x11-server: reattaching to different master device may lead to out-of-bounds memory access
- [BZ - 2257689](#) - CVE-2024-0408 xorg-x11-server: SELinux unlabeled GLX PBuffer
- [BZ - 2257690](#) - CVE-2024-0409 xorg-x11-server: SELinux context corruption



## CVEs

- [CVE-2023-5367](#)
- [CVE-2023-5380](#)
- [CVE-2023-6377](#)
- [CVE-2023-6478](#)
- [CVE-2023-6816](#)
- [CVE-2024-0229](#)
- [CVE-2024-0408](#)
- [CVE-2024-0409](#)
- [CVE-2024-21885](#)
- [CVE-2024-21886](#)


## References

- <https://access.redhat.com/security/updates/classification/#moderate>
- [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/8.10\\_release\\_notes/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/8.10_release_notes/index)


The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.




---

Quick Links 


---


Help 

---

Site Info 

---

Related Sites 

 Partial system outage



- About Red Hat
- Jobs
- Events
- Locations
- Contact Red Hat
- Red Hat Blog
- Inclusion at Red Hat
- Cool Stuff Store
- Red Hat Summit

---

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)