



Red Hat Product Errata    RHSA-2025:22742 - Security Advisory

# RHSA-2025:22742 - Security Advisory

Issued: 2025-12-04    Updated: 2025-12-04

[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 9.4 Extended Update Support.

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: xmayland: Use-after-free in XPresentNotify structure creation (CVE-2025-62229)
- xorg: xwayland: Use-after-free in Xkb client resource removal (CVE-2025-62230)
- xorg: xmayland: Value overflow in XkbSetCompatMap() (CVE-2025-62231)

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.

## 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 - Extended Update Support 9.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.4 x86\_64
- Red Hat CodeReady Linux Builder for x86\_64 - Extended Update Support 9.4 x86\_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.4 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x

## Fixes

- [BZ - 2402649](#) [↗](#) - CVE-2025-62229 xorg: xmayland: Use-after-free in XPresentNotify structure creation
- [BZ - 2402653](#) [↗](#) - CVE-2025-62230 xorg: xwayland: Use-after-free in Xkb client resource removal
- [BZ - 2402660](#) [↗](#) - CVE-2025-62231 xorg: xmayland: Value overflow in XkbSetCompatMap()

## CVEs

- [CVE-2025-62229](#) [↗](#)
- [CVE-2025-62230](#) [↗](#)
- [CVE-2025-62231](#) [↗](#)

## References

- <https://access.redhat.com/security/updates/classification/#moderate> [↗](#)

---

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 [↕](#)

---

 Loading



[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](#)