

[Red Hat Product Errata](#)    [RHSA-2025:20958 - Security Advisory](#)

# RHSA-2025:20958 - Security Advisory

Issued: 2025-11-11

Updated: 2025-11-11

[Overview](#)[Updated Packages](#)

## Synopsis

Important: tigervnc security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for tigervnc is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Important. 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

Virtual Network Computing (VNC) is a remote display system which allows users to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients.

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 9 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64

## 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/#important> 

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](#)