



Red Hat Product Errata    RHSA-2024:0614 - Security Advisory

# RHSA-2024:0614 - Security Advisory

Issued: 2024-01-30    Updated: 2024-01-30

[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 9.0 Extended Update Support.

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-x11-server: Heap buffer overflow in DeviceFocusEvent and ProcXIQueryPointer (CVE-2023-6816)
- xorg-x11-server: reattaching to different master device may lead to out-of-bounds memory access (CVE-2024-0229)
- xorg-x11-server: heap buffer overflow in XISendDeviceHierarchyEvent (CVE-2024-21885)
- xorg-x11-server: heap buffer overflow in DisableDevice (CVE-2024-21886)

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 9.0 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.0 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x

## Fixes

- [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 - 2257691](#) - CVE-2023-6816 xorg-x11-server: Heap buffer overflow in DeviceFocusEvent and ProcXIQueryPointer

## CVEs

- [CVE-2023-6816](#)
- [CVE-2024-0229](#)
- [CVE-2024-21885](#)
- [CVE-2024-21886](#)

## 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



✓ All systems operational



[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](#)