

红帽产品勘误 [RHSA-2024:0607 - Security Advisory](#)

# RHSA-2024:0607 - Security Advisory

发布：2024-01-30 已更新：2024-01-30

[概述](#)[更新的软件包](#)

## 概述

Important: tigervnc security update

## 类型/严重性

Security Advisory: Important

### Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

[查看受影响的系统](#) [↗](#)

## 标题

An update for tigervnc is now available for Red Hat Enterprise Linux 8.

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.

## 描述

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.

## 解决方案





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

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

## 受影响的产品

- 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

## 修复

- 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

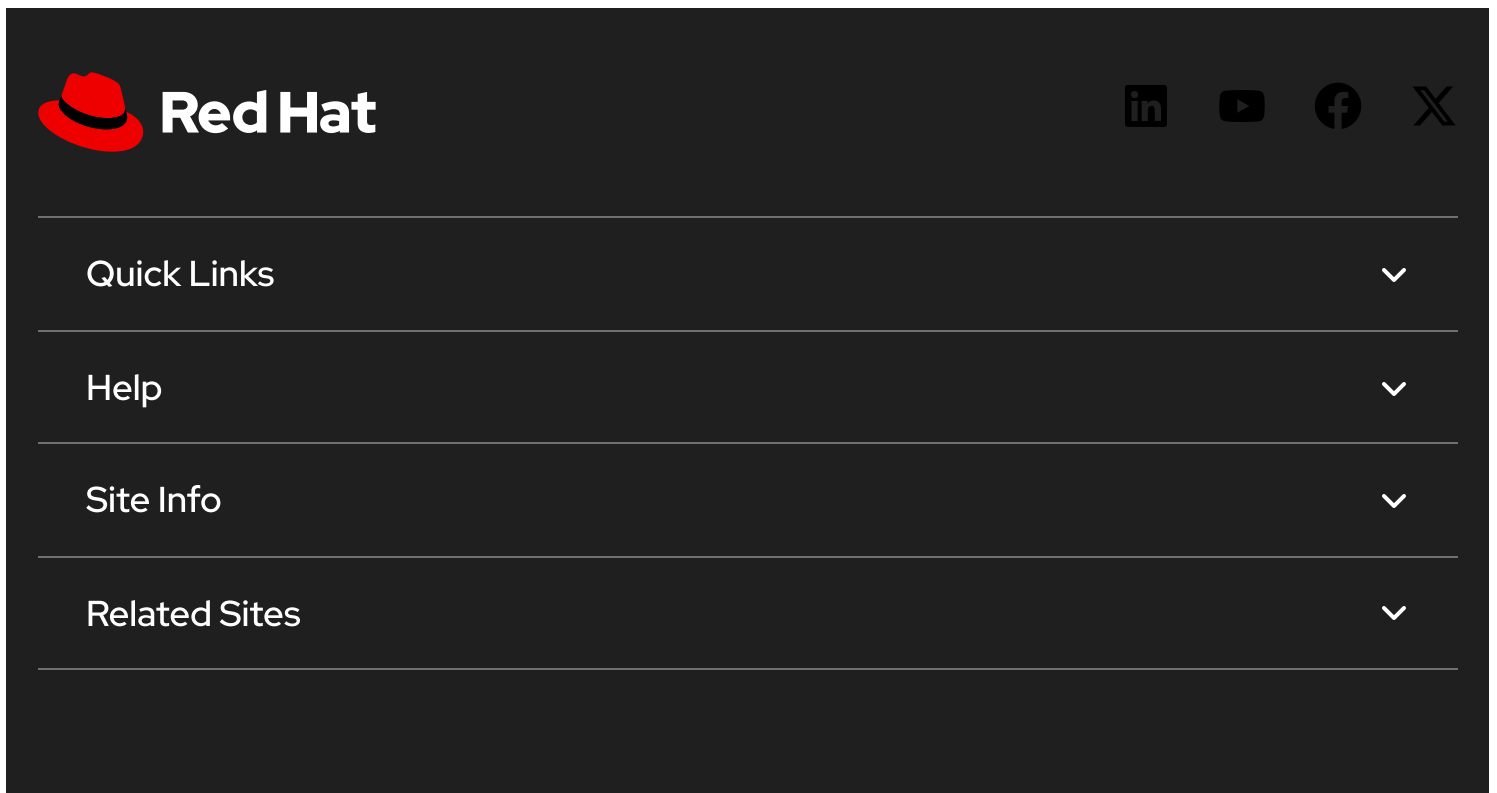
## CVE

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

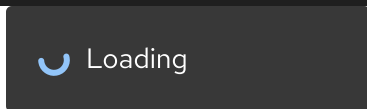
## 参考

- <https://access.redhat.com/security/updates/classification/#important>

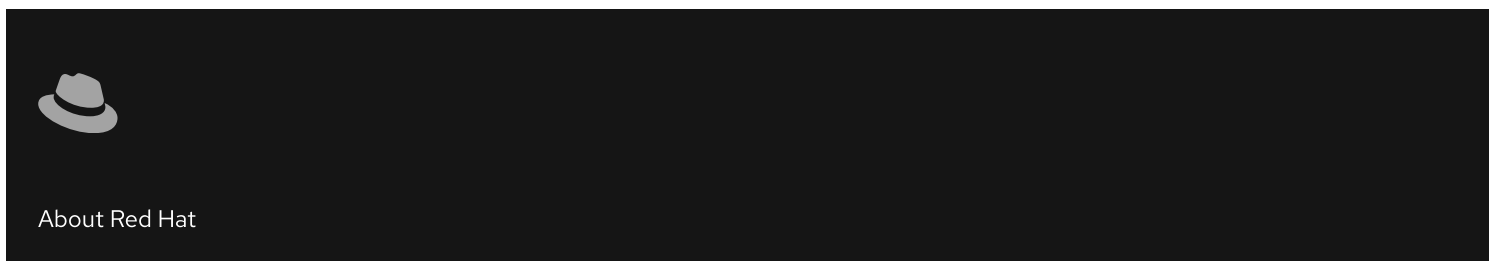
Red Hat 安全团队联络方式为 [secalert@redhat.com](mailto:secalert@redhat.com)。更多联络细节请参考 <https://access.redhat.com/security/team/contact/>。



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward-pointing chevron icon on the right: "Quick Links", "Help", "Site Info", and "Related Sites".



A dark grey rectangular box containing a blue circular loading spinner icon and the text "Loading".



A dark grey rectangular box containing a small grey hat icon on the left and the text "About Red Hat" below it.

[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](#)