



Red Hat Product Errata RHSA-2024:0006 - Security Advisory

RHSA-2024:0006 - Security Advisory

Issued: 2024-01-02 Updated: 2024-01-02

[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 7.

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: 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)

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 Server 7 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Enterprise Linux Desktop 7 x86_64
- Red Hat Enterprise Linux for IBM z Systems 7 s390x
- Red Hat Enterprise Linux for Power, big endian 7 ppc64
- Red Hat Enterprise Linux for Scientific Computing 7 x86_64
- Red Hat Enterprise Linux for Power, little endian 7 ppc64le
- Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le

Fixes

- [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

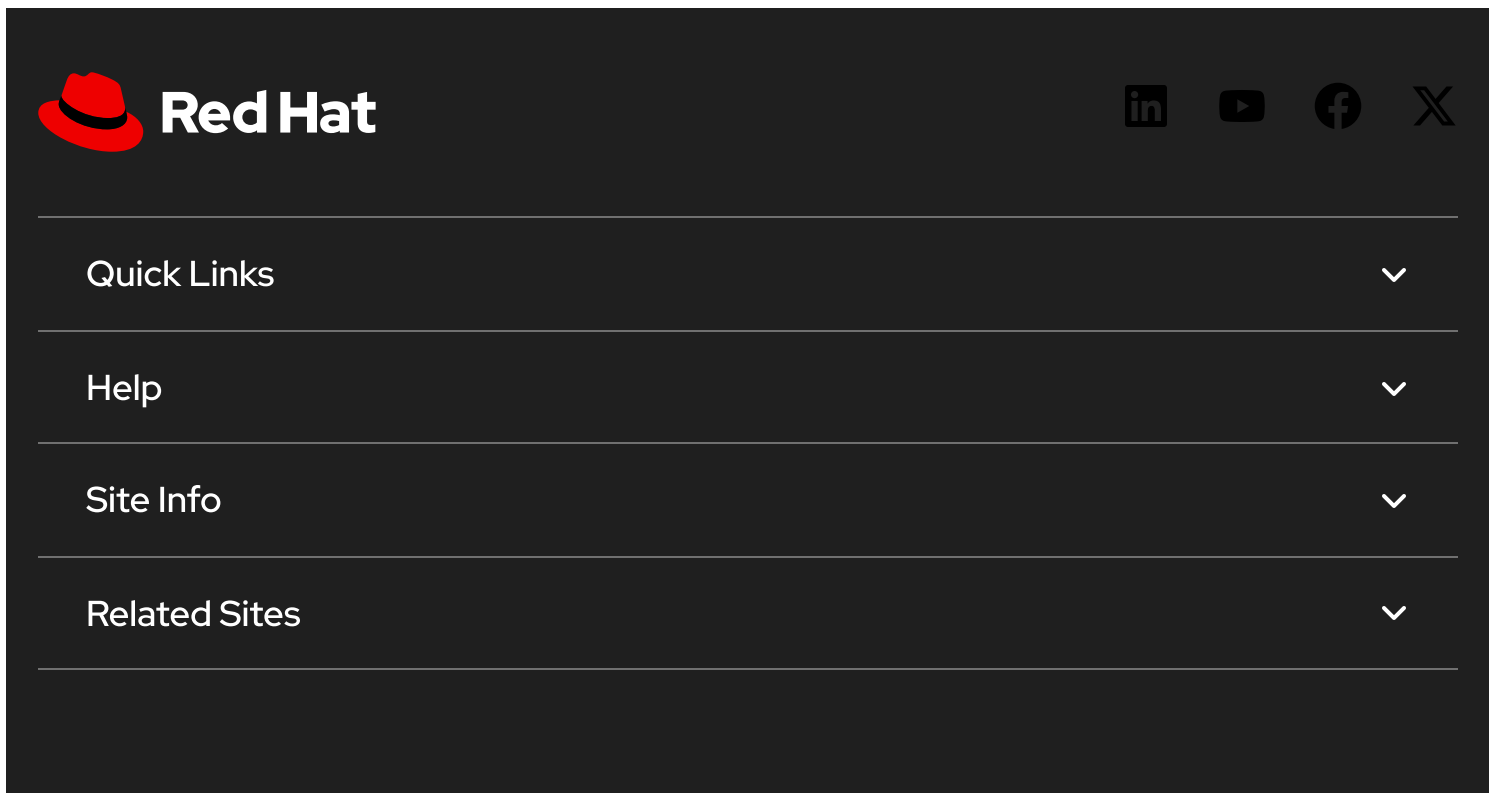
CVEs

- [CVE-2023-6377](#)
- [CVE-2023-6478](#)


References

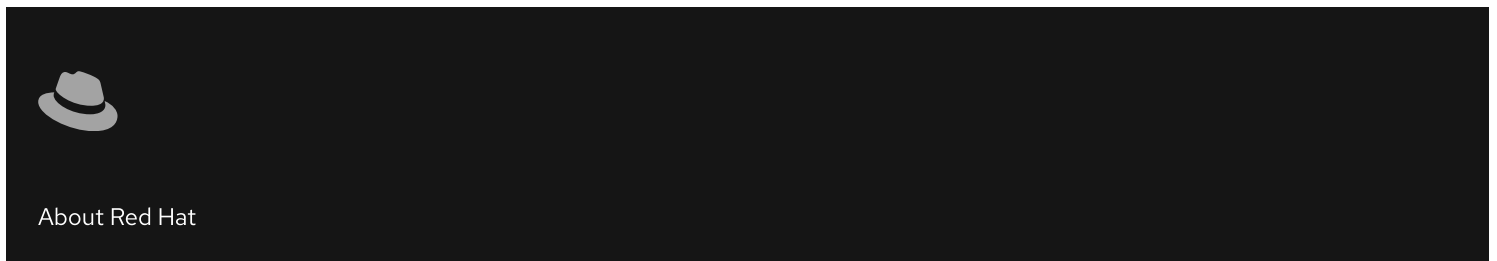
- <https://access.redhat.com/security/updates/classification/#important>

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



The image shows the Red Hat logo (a red fedora hat) and the text "Red Hat" in white on a dark background. To the right of the logo are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right. The menu items are separated by thin white horizontal lines.

 Partial system outage



The image shows a dark rectangular box with a white fedora hat icon on the left. Below the icon is the text "About Red Hat" in white.

[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](#)