



Red Hat Product Errata RHSA-2024:0020 - Security Advisory

RHSA-2024:0020 - 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 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: 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 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 - 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](#) 

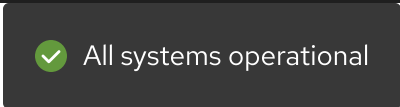
References

- <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 a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat icon) 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 notification box with a green checkmark icon on the left and the text "All systems operational" to its right.



The image shows a dark-themed footer navigation menu. It starts with a small grey hat icon. Below it is a list of links: "About Red Hat", "Jobs", "Events", "Locations", "Contact Red Hat", "Red Hat Blog", and "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](#)