



Red Hat Product Errata RHSA-2025:2866 - Security Advisory

RHSA-2025:2866 - Security Advisory

Issued: 2025-03-17 Updated: 2025-03-17

[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 8.2 Advanced 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):

- X.Org: Xwayland: Use-after-free of the root cursor (CVE-2025-26594)
- xorg: xwayland: Use-after-free in SynclnitTrigger() (CVE-2025-26601)
- xorg: xwayland: Use-after-free in PlayReleasedEvents() (CVE-2025-26600)
- xorg: xwayland: Use of uninitialized pointer in compRedirectWindow() (CVE-2025-26599)
- xorg: xwayland: Out-of-bounds write in CreatePointerBarrierClient() (CVE-2025-26598)
- xorg: xwayland: Buffer overflow in XkbChangeTypesOfKey() (CVE-2025-26597)
- xorg: xwayland: Heap overflow in XkbWriteKeySyms() (CVE-2025-26596)
- Xorg: xwayland: Buffer overflow in XkbVModMaskText() (CVE-2025-26595)

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 - AUS 8.2 x86_64

Fixes

- [BZ - 2345248](#) - CVE-2025-26594 X.Org: Xwayland: Use-after-free of the root cursor
- [BZ - 2345251](#) - CVE-2025-26601 xorg: xwayland: Use-after-free in SynclnitTrigger()
- [BZ - 2345252](#) - CVE-2025-26600 xorg: xwayland: Use-after-free in PlayReleasedEvents()
- [BZ - 2345253](#) - CVE-2025-26599 xorg: xwayland: Use of uninitialized pointer in compRedirectWindow()
- [BZ - 2345254](#) - CVE-2025-26598 xorg: xwayland: Out-of-bounds write in CreatePointerBarrierClient()
- [BZ - 2345255](#) - CVE-2025-26597 xorg: xwayland: Buffer overflow in XkbChangeTypesOfKey()
- [BZ - 2345256](#) - CVE-2025-26596 xorg: xwayland: Heap overflow in XkbWriteKeySyms()

- [BZ - 2345257](#) - CVE-2025-26595 Xorg: xwayland: Buffer overflow in XkbVModMaskText()


CVEs

- [CVE-2025-26594](#)
- [CVE-2025-26595](#)
- [CVE-2025-26596](#)
- [CVE-2025-26597](#)
- [CVE-2025-26598](#)
- [CVE-2025-26599](#)
- [CVE-2025-26600](#)
- [CVE-2025-26601](#)

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 hat) and the text "Red Hat" in white on a dark background. To the right of the logo are social media icons for LinkedIn, YouTube, Facebook, and X. Below these is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

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 and Do Not Sell or Share My Personal Information](#)