



Red Hat Product Errata    RHSA-2025:3976 - Security Advisory

## RHSA-2025:3976 - Security Advisory

Issued: 2025-04-17

Updated: 2025-04-17

[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 7 Extended Lifecycle 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: Buffer overflow in XkbVModMaskText() (CVE-2025-26595)
- xorg: xwayland: Heap overflow in XkbWriteKeySyms() (CVE-2025-26596)
- xorg: xwayland: Buffer overflow in XkbChangeTypesOfKey() (CVE-2025-26597)
- xorg: xwayland: Out-of-bounds write in CreatePointerBarrierClient()

(CVE-2025-26598)

- xorg: xwayland: Use of uninitialized pointer in compRedirectWindow()

(CVE-2025-26599)

- xorg: xwayland: Use-after-free in PlayReleasedEvents() (CVE-2025-26600)
- xorg: xwayland: Use-after-free in SynclnitTrigger() (CVE-2025-26601)

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

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

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

## Affected Products

- Red Hat Enterprise Linux Server 6 x86\_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86\_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386
- Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x

## 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](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[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](#)