RHSA-2025:2865 - Security Advisory

发布： 2025-03-17 已更新： 2025-03-17

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 8.4 Advanced Mission Critical Update Support, Red Hat Enterprise Linux 8.4 Telecommunications Update Service, and Red Hat Enterprise Linux 8.4 Update Services for SAP Solutions.

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):

- X.Org: Xwayland: Use-after-free of the root cursor (CVE-2025-26594)
- xorg: xwayland: Use-after-free in SyncInitTrigger() (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.

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 - Extended Update Support Extension 8.4 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64

修复

- 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 SyncInitTrigger()
- 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()

CVE

- CVE-2025-26594
- CVE-2025-26595
- CVE-2025-26596
- CVE-2025-26597
- CVE-2025-26598
- CVE-2025-26599
- CVE-2025-26600
- CVE-2025-26601

参考

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

---

Red Hat 安全团队联络方式为 secalert@redhat.com。 更多联络细节请参考 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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie preferences