RHSA-2025:12751 - Security Advisory

Issued: 2025-08-04 Updated: 2025-08-04

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 6 Extended Lifecycle Support - EXTENSION.

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: XTestSwapFakeInput stack overflow (CVE-2022-46340)
- xorg-x11-server: XIPassiveUngrab out-of-bounds access (CVE-2022-46341)
- xorg-x11-server: XvdiSelectVideoNotify use-after-free (CVE-2022-46342)
- xorg-x11-server: ScreenSaverSetAttributes use-after-free (CVE-2022-46343)
- xorg-x11-server: XIChangeProperty out-of-bounds access (CVE-2022-46344)
- xorg-x11-server: XkbGetKbdByName use-after-free (CVE-2022-4283)
- xorg-x11-server: DeepCopyPointerClasses use-after-free leads to privilege elevation (CVE-2023-0494)
- xorg-x11-server: X.Org Server Overlay Window Use-After-Free Local Privilege Escalation Vulnerability (CVE-2023-1393)
- xorg-x11-server: Out-of-bounds write in XIChangeDeviceProperty/RRChangeOutputProperty (CVE-2023-5367)
- xorg-x11-server: out-of-bounds memory read in RRChangeOutputProperty and RRChangeProviderProperty (CVE-2023-6478)
- xorg-x11-server: heap buffer overflow in XISendDeviceHierarchyEvent (CVE-2024-21885,ZDI-CAN-22744)
- xorg-x11-server: heap buffer overflow in DisableDevice (CVE-2024-21886,ZDI-CAN-22840)
- xorg-x11-server: reattaching to different master device may lead to out-of-bounds memory access (CVE-2024-0229,ZDI-CAN-22678)
- xorg-x11-server: Heap buffer overflow in DeviceFocusEvent and ProcXIQueryPointer (CVE-2023-6816)
- xorg-x11-server: Heap buffer overread/data leakage in ProcXIGetSelectedEvents (CVE-2024-31080)
- xorg-x11-server: Heap buffer overread/data leakage in ProcXIPassiveGrabDevice (CVE-2024-31081)
- xorg-x11-server: Use-after-free in ProcRenderAddGlyphs (CVE-2024-31083)
- xorg-x11-server: tigervnc: heap-based buffer overflow privilege escalation vulnerability (CVE-2024-9632)

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 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 - 2151755 - CVE-2022-46340 xorg-x11-server: XTestSwapFakeInput stack overflow
- BZ - 2151756 - CVE-2022-46341 xorg-x11-server: XIPassiveUngrab out-of-bounds access
- BZ - 2151757 - CVE-2022-46342 xorg-x11-server: XvdiSelectVideoNotify use-after-free
- BZ - 2151758 - CVE-2022-46343 xorg-x11-server: ScreenSaverSetAttributes use-after-free
- BZ - 2151760 - CVE-2022-46344 xorg-x11-server: XIChangeProperty out-of-bounds access
- BZ - 2151761 - CVE-2022-4283 xorg-x11-server: XkbGetKbdByName use-after-free
- BZ - 2165995 - CVE-2023-0494 xorg-x11-server: DeepCopyPointerClasses use-after-free leads to privilege elevation
- BZ - 2180288 - CVE-2023-1393 xorg-x11-server: X.Org Server Overlay Window Use-After-Free Local Privilege Escalation Vulnerability
- BZ - 2243091 - CVE-2023-5367 xorg-x11-server: Out-of-bounds write in XIChangeDeviceProperty/RRChangeOutputProperty
- BZ - 2253298 - CVE-2023-6478 xorg-x11-server: out-of-bounds memory read in RRChangeOutputProperty and RRChangeProviderProperty
- BZ - 2256540 - CVE-2024-21885 xorg-x11-server: heap buffer overflow in XISendDeviceHierarchyEvent
- BZ - 2256542 - CVE-2024-21886 xorg-x11-server: heap buffer overflow in DisableDevice
- BZ - 2256690 - CVE-2024-0229 xorg-x11-server: reattaching to different master device may lead to out-of-bounds memory access
- BZ - 2257691 - CVE-2023-6816 xorg-x11-server: Heap buffer overflow in DeviceFocusEvent and ProcXIQueryPointer
- BZ - 2271997 - CVE-2024-31080 xorg-x11-server: Heap buffer overread/data leakage in ProcXIGetSelectedEvents
- BZ - 2271998 - CVE-2024-31081 xorg-x11-server: Heap buffer overread/data leakage in ProcXIPassiveGrabDevice

- BZ - 2272000 - CVE-2024-31083 xorg-x11-server: Use-after-free in ProcRenderAddGlyphs
- BZ - 2317233 - CVE-2024-9632 xorg-x11-server: tigervnc: heap-based buffer overflow privilege escalation vulnerability

CVEs

- CVE-2022-4283
- CVE-2022-46340
- CVE-2022-46341
- CVE-2022-46342
- CVE-2022-46343
- CVE-2022-46344
- CVE-2023-0494
- CVE-2023-1393
- CVE-2023-5367
- CVE-2023-6478
- CVE-2023-6816
- CVE-2024-0229
- CVE-2024-9632
- CVE-2024-21885
- CVE-2024-21886
- CVE-2024-31080
- CVE-2024-31081
- CVE-2024-31083

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/.

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 and Opt-Out Rights