RHSA-2025:7458 - Security Advisory

发布： 2025-05-13 已更新： 2025-05-13

概述

更新的软件包

概述

Important: xorg-x11-server-Xwayland 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 xorg-x11-server-Xwayland is now available for Red Hat Enterprise Linux 10.

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

Xwayland is an X server for running X clients under Wayland.

Security Fix(es):

- xorg-x11-server: tigervnc: heap-based buffer overflow privilege escalation vulnerability (CVE-2024-9632)
- 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 10 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64

- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64

修复

- BZ - 2317233 - CVE-2024-9632 xorg-x11-server: tigervnc: heap-based buffer overflow privilege escalation vulnerability
- 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()
- RHEL-66317 - Drop unused build dependencies in Xwayland in el10
- RHEL-78562 - Please backport Fedora 40 changes in xorg-x11-server-Xwayland if needed (2025-02-09)

CVE

- CVE-2024-9632
- 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/。

Red Hat

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