CVE-2025-62229

VEX

Public on October 29, 2025

Last modified: April 20, 2026 at 1:50:11 PM UTC

MODERATE

Moderate severity

What does this mean?

7.3

CVSS v3 Score Breakdown

Jump to section

Description | Statement | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | Acknowledgements | FAQ

Description

A flaw was found in the X.Org X server and Xwayland when processing X11 Present extension notifications. Improper error handling during notification creation can leave dangling pointers that lead to a use-after-free condition. This can cause memory corruption or a crash, potentially allowing an attacker to execute arbitrary code or cause a denial of service.

Statement

The Red Hat Product Security team has rated this vulnerability as Moderate. The flaw is a use-after-free in X11 Present notification handling that could lead to integrity and availability impacts if exploited. Moreover, the X.Org server does not run with root privileges in Red Hat Enterprise Linux 8 and 9, limiting the potential impact and preventing system-wide compromise.

Mitigation

Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Additional information

- Bugzilla 2402649: xorg: xmayland: Use-after-free in XPresentNotify structure creation
- CWE-416: Use After Free

External references

- https://www.cve.org/CVERecord?id=CVE-2025-62229
- https://nvd.nist.gov/vuln/detail/CVE-2025-62229
- https://lists.x.org/archives/xorg-announce/2025-October/003635.html

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	xorg-x11-server-Xwayland
State	Fixed
Justification	None
Errata	RHSA-2025:19435
Release Date	November 3, 2025

Products / Services	Red Hat Enterprise Linux 10
Components	xorg-x11-server-Xwayland
State	Fixed
Justification	None
Errata	RHSA-2025:21035
Release Date	November 11, 2025

Products / Services	Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION
Components	tigervnc Important
State	Fixed

1 of 5

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	7.3	N/A	N/A
Attack Vector	Local	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	Low	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	Low	N/A	N/A
Integrity Impact	High	N/A	N/A
Availability Impact	High	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

Acknowledgements

Red Hat would like to thank Jan-Niklas Sohn (Trend Micro Zero Day Initiative) for reporting this issue.

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors?
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?
- What can I do if my product is listed as "Will not fix"?
- What can I do if my product is listed as "Fix deferred"?
- What is a mitigation?
- I have a Red Hat product but it is not in the above list, is it affected?
- Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?
- My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: April 20, 2026 at 1:50:11 PM UTC