

X.Org Security Advisory: multiple security issues X.Org X server and Xwayland

Olivier Fourdan [ofourdan at redhat.com](mailto:ofourdan@redhat.com)

Tue Oct 28 13:22:18 UTC 2025

- Previous message (by thread): [\[ANNOUNCE\] libdrm 2.4.127](#)
- Next message (by thread): [\[ANNOUNCE\] xorg-server 21.1.19](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

=====

X.Org Security Advisory: October 28, 2025

Issues in X.Org X server prior to 21.1.18 and Xwayland prior to 24.1.8

=====

Multiple issues have been found in the X server and Xwayland implementations published by X.Org for which we are releasing security fixes for in xorg-server-21.1.19 and xwayland-24.1.9.

1) CVE-2025-62229: Use-after-free in XPresentNotify structures creation

Using the X11 Present extension, when processing and adding the notifications after presenting a pixmap, if an error occurs, a dangling pointer may be left in the error code path of the function causing a use-after-free when eventually destroying the notification structures later.

Introduced in: Xorg 1.15

Fixed in: xorg-server-21.1.19 and xwayland-24.1.9

Fix: <https://gitlab.freedesktop.org/xorg/xserver/-/commit/5a4286b1>

Found by: Jan-Niklas Sohn working with Trend Micro Zero Day Initiative.

2) CVE-2025-62230: Use-after-free in Xkb client resource removal

When removing the Xkb resources for a client, the function XkbRemoveResourceClient() will free the XkbInterest data associated with the device, but not the resource associated with it.

As a result, when the client terminates, the resource delete function triggers a use-after-free.

Introduced in: X11R6

Fixed in: xorg-server-21.1.19 and xwayland-24.1.9

Fix: <https://gitlab.freedesktop.org/xorg/xserver/-/commit/99790a2c>

<https://gitlab.freedesktop.org/xorg/xserver/-/commit/10c94238>

Found by: Jan-Niklas Sohn working with Trend Micro Zero Day Initiative.

3) CVE-2025-62231: Value overflow in Xkb extension XkbSetCompatMap()

The XkbCompatMap structure stores some of its values using an unsigned short, but fails to check whether the sum of the input data might overflow the maximum unsigned short value.

Introduced in: X11R6

Fixed in: xorg-server-21.1.19 and xwayland-24.1.9

Fix: <https://gitlab.freedesktop.org/xorg/xserver/-/commit/475d9f49>

Found by: Jan-Niklas Sohn working with Trend Micro Zero Day Initiative.

X.Org thanks all of those who reported and fixed these issues, and those who helped with the review and release of this advisory and these fixes.

----- next part -----

A non-text attachment was scrubbed...

Name: OpenPGP_0x14706DBE1E4B4540.asc

Type: application/pgp-keys

Size: 2988 bytes

Desc: OpenPGP public key

URL: <<https://lists.x.org/archives/xorg-announce/attachments/20251028/ff11c77e/attachment.key>>

----- next part -----

A non-text attachment was scrubbed...

Name: OpenPGP_signature.asc

Type: application/pgp-signature

Size: 203 bytes

Desc: OpenPGP digital signature

URL: <<https://lists.x.org/archives/xorg-announce/attachments/20251028/ff11c77e/attachment.sig>>

-
- Previous message (by thread): [[ANNOUNCE](#)] [libdrm 2.4.127](#)
 - Next message (by thread): [[ANNOUNCE](#)] [xorg-server 21.1.19](#)
 - **Messages sorted by:** [[date](#)] [[thread](#)] [[subject](#)] [[author](#)]

[More information about the xorg-announce mailing list](#)