

X.Org Security Advisory: Issues in X.Org X server prior to 21.1.10 and Xwayland prior to 23.2.3

Peter Hutterer [peter.hutterer at who-t.net](mailto:peter.hutterer@who-t.net)

Wed Dec 13 02:02:01 UTC 2023

- Next message (by thread): [\[ANNOUNCE\] xorg-server 21.1.10](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

X.Org Security Advisory: December 13, 2023

Issues in X.Org X server prior to 21.1.10 and Xwayland prior to 23.2.3
 =====

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-21.1.10 and xwayland-23.2.3.

- 1) CVE-2023-6377 can be triggered by forcing a logical device change on a device with buttons which will result in an out-of-bounds memory write.
- 2) CVE-2023-6478 can be triggered by sending a specially crafted request RRChangeProviderProperty or RRChangeOutputProperty. This will trigger an integer overflow and lead to disclosure of information.

1) CVE-2023-6377: X.Org server: Out-of-bounds memory write in XKB button actions

Introduced in: xorg-server-1.6.0 (2009)

Fixed in: xorg-server-21.1.10 and xwayland-23.2.3

Fix:

<https://gitlab.freedesktop.org/xorg/xserver/-/commit/0c1a93d319558fe3ab2d94f51d174b4f93810afd>

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

A device has XKB button actions for each button on the device. When a logical device switch happens (e.g. moving from a touchpad to a mouse), the server re-calculates the information available on the respective master device (typically the Virtual Core Pointer). This re-calculation only allocated enough memory for a single XKB action rather instead of enough for the newly active physical device's number of button. As a result, querying or changing the XKB button actions results in out-of-bounds memory reads and writes.

This may lead to local privilege escalation if the server is run as root or remote code execution (e.g. x11 over ssh).

xorg-server-21.1.10 and xwayland-23.2.3 have been patched to fix this issue.

2) CVE-2023-6478: X.Org server: Out-of-bounds memory read in RRChangeOutputProperty and RRChangeProviderProperty

Introduced in: xorg-server-1.4.0 (2007) and xorg-server-1.13.0 (2012), respectively

Fixed in: xorg-server-21.1.10 and xwayland-23.2.3

Fix:

<https://gitlab.freedesktop.org/xorg/xserver/-/commit/14f480010a93ff962fef66a16412fafff81ad632>

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

This fixes an OOB read and the resulting information disclosure.

Length calculation for the request was clipped to a 32-bit integer. With the correct stuff->nUnits value the expected request size was truncated, passing the REQUEST_FIXED_SIZE check.

The server then proceeded with reading at least stuff->nUnits bytes (depending on stuff->format) from the request and stuffing whatever it finds into the property. In the process it would also allocate at least stuff->nUnits bytes, i.e. 4GB.

See also CVE-2022-46344 where this issue was fixed for other requests.

xorg-server-21.1.10 and xwayland-23.2.3 have been patched to fix this issue.

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: signature.asc

Type: application/pgp-signature

Size: 195 bytes

Desc: not available

URL: <<https://lists.x.org/archives/xorg-announce/attachments/20231213/85470162/attachment.sig>>

-
- Next message (by thread): [[ANNOUNCE](#)] [xorg-server 21.1.10](#)
 - **Messages sorted by:** [[date](#)] [[thread](#)] [[subject](#)] [[author](#)]

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