



Bug 2451109 (CVE-2026-34001) - CVE-2026-34001 xorg: xwayland: X.Org X server: Use-after-free vulnerability leads to server crash and potential memory corruption

Keywords: Security

Reported: 2026-03-25 07:00 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-04-23 14:17 UTC ([History](#))

Alias: CVE-2026-34001

CC List: 1 user ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-03-25 07:00:31 UTC

[Description](#)

Use-after-free vulnerability in the XSYNC fence triggering logic of the X.Org X server. The flaw occurs in miSyncTriggerFence() while walking the list of fences to trigger: calling TriggerFence() for the current entry can invoke SyncAwaitTriggerFired(), which frees the entire await resource. This free operation removes all triggers from the await object, including subsequent list entries that miSyncTriggerFence() may still attempt to process, resulting in a use-after-free. An attacker with access to the X11 server can trigger the bug without user interaction, potentially crashing the server and, in some configurations, enabling

memory corruption with higher impact.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

