



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: 2026-04-29 13:07 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) |
|-------------|--------------------------------|
| | |

Links

| System | ID | Private | Priority | Status | Summary | Last Updated |
|------------------------|---------------------------------|---------|----------|--------|---------|-------------------------|
| Red Hat Product Errata | RHSA-2026:10739 | 0 | None | None | None | 2026-04-27 08:29:52 UTC |
| Red Hat Product Errata | RHSA-2026:11352 | 0 | None | None | None | 2026-04-28 11:21:05 UTC |
| Red Hat Product Errata | RHSA-2026:11369 | 0 | None | None | None | 2026-04-28 14:53:17 UTC |

| | | | | | | |
|------------------------|---------------------------------|---|------|------|------|-------------------------|
| Red Hat Product Errata | RHSA-2026:11388 | 0 | None | None | None | 2026-04-28 17:58:04 UTC |
| Red Hat Product Errata | RHSA-2026:11656 | 0 | None | None | None | 2026-04-29 12:01:25 UTC |
| Red Hat Product Errata | RHSA-2026:11692 | 0 | None | None | None | 2026-04-29 13:07:52 UTC |

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.

errata-xmlrpc 2026-04-27 08:29:51 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via [RHSA-2026:10739](#) <https://access.redhat.com/errata/RHSA-2026:10739>

errata-xmlrpc 2026-04-28 11:21:04 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via [RHSA-2026:11352](#) <https://access.redhat.com/errata/RHSA-2026:11352>

errata-xmlrpc 2026-04-28 14:53:16 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:11369 <https://access.redhat.com/errata/RHSA-2026:11369>

errata-xmlrpc 2026-04-28 17:58:03 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:11388 <https://access.redhat.com/errata/RHSA-2026:11388>

errata-xmlrpc 2026-04-29 12:01:23 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:11656 <https://access.redhat.com/errata/RHSA-2026:11656>

errata-xmlrpc 2026-04-29 13:07:51 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:11692 <https://access.redhat.com/errata/RHSA-2026:11692>

Note

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

