



## Bug 2451113 (CVE-2026-34003) - CVE-2026-34003 xorg: xwayland: X.Org X server: Information exposure and denial of service via out-of-bounds memory access

**Keywords:**  ✕ ▼

**Reported:** 2026-03-25 07:19 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-29 13:07 UTC ([History](#))

**Alias:** CVE-2026-34003

**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 DevOps Team

**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	<a href="#">RHSA-2026:10739</a>	0	None	None	None	2026-04-27 08:29:54 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:11352</a>	0	None	None	None	2026-04-28 11:21:05 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:11369</a>	0	None	None	None	2026-04-28 14:53:19 UTC

Red Hat Product Errata	<a href="#">RHSA-2026:11388</a>	0	None	None	None	2026-04-28 17:58:04 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:11656</a>	0	None	None	None	2026-04-29 12:01:28 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:11692</a>	0	None	None	None	2026-04-29 13:07:54 UTC

OSIDB Bzimport  2026-03-25 07:19:37 UTC[Description](#)

Out-of-bounds memory access vulnerability in the XKB key types request validation of the X.Org X server. The function `CheckKeyTypes()` loops over elements derived from the client's request but does not perform adequate bounds checking to guarantee that subsequent reads remain within the request payload. A specially crafted request can cause `CheckKeyTypes()` to read uninitialized memory past the end of the request data, potentially leading to information exposure and/or a server crash. In certain configurations (as indicated by the submitted impact notes), this memory-safety flaw may be exploitable for higher impact outcomes.

errata-xmlrpc 2026-04-27 08:29:53 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 11:21:03 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 14:53:18 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 12:01:24 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 13:07:53 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.

