



## 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:** Security

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

**Status:** NEW

**Modified:** 2026-04-23 14:20 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](#))

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.

---

Note

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

