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

Status: NEW

Alias: CVE-2026-34003

Product: Security Response

Component: vulnerability

Version: unspecified

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

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

Modified: 2026-04-27 08:29 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

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 08:29:54 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

Note

You need to log in before you can comment on or make changes to this bug.