



Bug 2345255 (CVE-2025-26597) - CVE-2025-26597 xorg: xwayland: Buffer overflow in XkbChangeTypesOfKey()

Keywords:

Reported: 2025-02-12 14:23 UTC by OSIDB Bzimport

Status: NEW

Modified: 2025-10-13 12:12 UTC ([History](#))

Alias: CVE-2025-26597

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

Deadline: 2025-02-25

Fixed In Version:

Product: Security Response

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

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: [2349376](#) [2349377](#) [2349378](#)

Blocks:


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

Attachments [\(Terms of Use\)](#)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:2500	0	None	None	None	2025-03-10 12:37:00 UTC
Red Hat Product Errata	RHSA-2025:2502	0	None	None	None	2025-03-10 12:46:07 UTC
Red Hat	RHSA-2025:2861	0	None	None	None	2025-03-17

Product Errata						01:28:48 UTC
Red Hat Product Errata	RHSA-2025:2862	0	None	None	None	2025-03-17 01:27:47 UTC
Red Hat Product Errata	RHSA-2025:2865	0	None	None	None	2025-03-17 01:36:11 UTC
Red Hat Product Errata	RHSA-2025:2866	0	None	None	None	2025-03-17 01:14:00 UTC
Red Hat Product Errata	RHSA-2025:2873	0	None	None	None	2025-03-17 01:37:43 UTC
Red Hat Product Errata	RHSA-2025:2874	0	None	None	None	2025-03-17 01:46:11 UTC
Red Hat Product Errata	RHSA-2025:2875	0	None	None	None	2025-03-17 01:44:08 UTC
Red Hat Product Errata	RHSA-2025:2879	0	None	None	None	2025-03-17 03:11:22 UTC
Red Hat Product Errata	RHSA-2025:2880	0	None	None	None	2025-03-17 04:20:07 UTC
Red Hat Product Errata	RHSA-2025:3976	0	None	None	None	2025-04-17 06:35:56 UTC
Red Hat Product Errata	RHSA-2025:7163	0	None	None	None	2025-05-13 10:14:15 UTC
Red Hat Product Errata	RHSA-2025:7165	0	None	None	None	2025-05-13 10:15:21 UTC
Red Hat Product Errata	RHSA-2025:7458	0	None	None	None	2025-05-13 15:55:12 UTC

OSIDB Bzimport  2025-02-12 14:23:50 UTC[Description](#)

If XkbChangeTypesOfKey() is called with 0 group, it will resize the key symbols table to 0 but leave the key actions unchanged.

If later, the same function is called with a non-zero value of groups, this will cause a buffer overflow because the key actions are of the wrong size.

errata-xmlrpc 2025-03-10 12:36:59 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:2500 <https://access.redhat.com/errata/RHSA-2025:2500>

errata-xmlrpc 2025-03-10 12:46:06 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2025:2502 <https://access.redhat.com/errata/RHSA-2025:2502>

errata-xmlrpc 2025-03-17 01:13:59 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:2866 <https://access.redhat.com/errata/RHSA-2025:2866>

errata-xmlrpc 2025-03-17 01:27:46 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.8 Extended Update Support

Via RHSA-2025:2862 <https://access.redhat.com/errata/RHSA-2025:2862>

2025:2862

errata-xmlrpc 2025-03-17 01:28:48 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:2861 <https://access.redhat.com/errata/RHSA-2025:2861>

errata-xmlrpc 2025-03-17 01:36:10 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support

Red Hat Enterprise Linux 8.4 Telecommunications Update Service

Red Hat Enterprise Linux 8.4 Update Services for SAP Solutions

Via RHSA-2025:2865 <https://access.redhat.com/errata/RHSA-2025:2865>

errata-xmlrpc 2025-03-17 01:37:42 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:2873 <https://access.redhat.com/errata/RHSA-2025:2873>

errata-xmlrpc 2025-03-17 01:44:07 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:2875 <https://access.redhat.com/errata/RHSA-2025:2875>

errata-xmlrpc 2025-03-17 01:46:10 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2025:2874 <https://access.redhat.com/errata/RHSA-2025:2874>

errata-xmlrpc 2025-03-17 03:11:21 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:2879 <https://access.redhat.com/errata/RHSA-2025:2879>

errata-xmlrpc 2025-03-17 04:20:06 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support

Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions

Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:2880 <https://access.redhat.com/errata/RHSA-2025:2880>

errata-xmlrpc 2025-04-17 06:35:55 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION

Via RHSA-2025:3976 <https://access.redhat.com/errata/RHSA-2025:3976>

errata-xmlrpc 2025-05-13 10:14:14 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:7163 <https://access.redhat.com/errata/RHSA-2025:7163>

errata-xmlrpc 2025-05-13 10:15:20 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2025:7165 <https://access.redhat.com/errata/RHSA-2025:7165>

errata-xmlrpc 2025-05-13 15:55:11 UTC

[Comment 17](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via RHSA-2025:7458 <https://access.redhat.com/errata/RHSA-2025:7458>

Note

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

