Bug 2345257 (CVE-2025-26595) - CVE-2025-26595 Xorg: xwayland: Buffer overflow in XkbVModMaskText()

Keywords: Security

Status: NEW

Alias: CVE-2025-26595

Deadline: 2025-02-25

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2349373~~ ~~2349374~~ ~~2349375~~

Blocks:

TreeView+ depends on / blocked

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

Modified: 2025-10-13 12:12 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-2025:2500	0	None	None	None	2025-03-10 12:37:03 UTC
Red Hat Product Errata	RHSA-2025:2502	0	None	None	None	2025-03-10 12:46:10 UTC
Red Hat	RHSA-2025:2861	0	None	None	None	2025-03-17

Product Errata						01:28:45 UTC
Red Hat Product Errata	RHSA-2025:2862	0	None	None	None	2025-03-17 01:27:50 UTC
Red Hat Product Errata	RHSA-2025:2865	0	None	None	None	2025-03-17 01:36:13 UTC
Red Hat Product Errata	RHSA-2025:2866	0	None	None	None	2025-03-17 01:14:01 UTC
Red Hat Product Errata	RHSA-2025:2873	0	None	None	None	2025-03-17 01:37:45 UTC
Red Hat Product Errata	RHSA-2025:2874	0	None	None	None	2025-03-17 01:46:13 UTC
Red Hat Product Errata	RHSA-2025:2875	0	None	None	None	2025-03-17 01:44:10 UTC
Red Hat Product Errata	RHSA-2025:2879	0	None	None	None	2025-03-17 03:11:23 UTC
Red Hat Product Errata	RHSA-2025:2880	0	None	None	None	2025-03-17 04:20:09 UTC
Red Hat Product Errata	RHSA-2025:3976	0	None	None	None	2025-04-17 06:35:58 UTC
Red Hat Product Errata	RHSA-2025:7163	0	None	None	None	2025-05-13 10:14:17 UTC
Red Hat Product Errata	RHSA-2025:7165	0	None	None	None	2025-05-13 10:15:28 UTC
Red Hat Product Errata	RHSA-2025:7458	0	None	None	None	2025-05-13 15:55:14 UTC

OSIDB Bzimport 2025-02-12 14:23:56 UTC Description

The code in XkbVModMaskText() allocates a fixed sized buffer on the
stack and copies the names of the virtual modifiers to that buffer.

The code however fails to check the bounds of the buffer correctly and
would copy the data regardless of the size, which may lead to a buffer
overflow.

errata-xmlrpc 2025-03-10 12:37:02 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 12:46:09 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 01:14:00 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 01:27:49 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

errata-xmlrpc 2025-03-17 01:28:45 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 01:36:13 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 01:37:44 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 01:44:09 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 01:46:12 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 03:11:22 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 04:20:08 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 06:35:57 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 10:14:16 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 10:15:27 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 15:55:13 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.