Xorg: xwayland: buffer overflow in xkbvmodmasktext()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-26595
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-25 16:15:38 UTC
Updated	2026-04-06 13:17:15 UTC
Description	A buffer overflow flaw was found in X.Org and Xwayland. The code in XkbVModMaskText() allocates a fixed-sized buffer or

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000210000 probability, percentile 0.057310000 (date 2026-04-07)

Problem Types: CWE-121 | CWE-787 | CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Tigervnc	Tigervnc	-	All	All	All
Application	X.org	Xwayland	All	All	All	All
Application	X.org	X Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platf
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:24.1.5-3.el10_0 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION	unaffected 0:1.1.0-25.el6_10 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:1.8.0-36.el7_9 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:1.20.4-30.el7_9 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:1.13.1-15.el8_10 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:1.9.0-15.el8_2.13 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:1.11.0-8.el8_4.12 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Telecommunications Update Service	unaffected 0:1.11.0-8.el8_4.12 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Update Services For SAP Solutions	unaffected 0:1.11.0-8.el8_4.12 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:1.12.0-6.el8_6.13 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:1.12.0-6.el8_6.13 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:1.12.0-6.el8_6.13 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Extended Update Support	unaffected 0:1.12.0-15.el8_8.12 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.14.1-1.el9_5.1 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.20.11-28.el9_6 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:23.2.7-3.el9_6 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:1.11.0-22.el9_0.13 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Extended Update Support	unaffected 0:1.12.0-14.el9_2.10 * rpm	Not s
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:1.13.1-8.el9_4.5 * rpm	Not s

CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not s
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not s

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:2879	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:3976	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:7163	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:7165	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:2502	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2861	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2874	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2862	secalert@redhat.com	access.redhat.com	Third Party
lists.debian.org/debian-lts-announce/2025/02/msg00036.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2025:2866	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2873	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2865	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2500	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2880	secalert@redhat.com	access.redhat.com	Third Party
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Trac
access.redhat.com/errata/RHSA-2025:7458	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-26595	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:2875	secalert@redhat.com	access.redhat.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-02-12T14:15:00.929Z	Reported to Red Hat.
CNA	2025-02-25T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment

meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

There are currently no legacy QID mappings associated with this CVE.