Xorg: xwayland: use-after-free in xkb client resource removal

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

Summary

CVE	CVE-2025-62230
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-30 06:15:45 UTC
Updated	2026-04-20 14:16:15 UTC
Description	A flaw was discovered in the X.Org X server's X Keyboard (Xkb) extension when handling client resource cleanup. The soft

Risk And Classification

Primary CVSS: v3.1 7.3 HIGH from secalert@redhat.com

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

EPSS: 0.000100000 probability, percentile 0.012260000 (date 2026-04-21)

Problem Types: CWE-416 | CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

Low

vailability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Pla
CNA	X.Org	Xwayland	affected 24.1.9 semver	No
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:24.1.5-5.el10_0 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:24.1.5-5.el10_1 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION	unaffected 0:1.1.0-25.el6_10.15 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:1.20.4-33.el7_9 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:1.8.0-36.el7_9.3 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:21.1.3-19.el8_10 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:1.20.11-27.el8_10 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:1.15.0-8.el8_10 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:1.9.0-15.el8_2.15 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:1.20.6-5.el8_2 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:1.11.0-8.el8_4.14 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:1.20.10-3.el8_4 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:1.11.0-8.el8_4.14 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:1.20.10-3.el8_4 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:1.12.0-6.el8_6.15 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:1.20.11-6.el8_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:21.1.3-2.el8_6.5 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:1.12.0-6.el8_6.15 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:1.20.11-6.el8_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:21.1.3-2.el8_6.5 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:1.12.0-6.el8_6.15 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:1.20.11-6.el8_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:21.1.3-2.el8_6.5 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:1.12.0-15.el8_8.16 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:1.20.11-17.el8_8 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:21.1.3-12.el8_8 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:1.12.0-15.el8_8.16 * rpm	No

CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:1.20.11-17.el8_8 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:21.1.3-12.el8_8 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.20.11-32.el9_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.14.1-9.el9_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:23.2.7-5.el9_6 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.15.0-6.el9_7 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:23.2.7-5.el9_7 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.20.11-32.el9_7 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:1.11.0-22.el9_0.16 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:1.20.11-12.el9_0 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:21.1.3-4.el9_0 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:1.12.0-14.el9_2.13 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:1.20.11-19.el9_2 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:21.1.3-9.el9_2 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:1.13.1-8.el9_4.8 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:1.20.11-27.el9_4 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:22.1.9-7.el9_4 * rpm	No
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	No

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:22040	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0035	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19435	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:20960	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2025/10/28/7	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
access.redhat.com/errata/RHSA-2025:22041	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0036	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22056	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:20958	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22167	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19434	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:20961	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22096	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19489	secalert@redhat.com	access.redhat.com	

access.redhat.com/errata/RHSA-2025:22164	secalert@redhat.com	access.redhat.com	
lists.x.org/archives/xorg-announce/2025-October/003635.html	secalert@redhat.com	lists.x.org	
access.redhat.com/errata/RHSA-2025:22753	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22077	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22055	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-62230	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21035	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0033	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22729	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19909	secalert@redhat.com	access.redhat.com	
lists.debian.org/debian-lts-announce/2025/10/msg00033.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:22742	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0034	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19623	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22364	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22667	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19432	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22426	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22051	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22365	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0031	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:22427	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19433	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Jan-Niklas Sohn (Trend Micro Zero Day Initiative) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-10-09T06:00:07.571Z	Reported to Red Hat.

CNA	2025-10-29T00:00:00.000Z	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, applicability to widespread installation base or stability.

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