



Bug 2317233 (CVE-2024-9632) - CVE-2024-9632 xorg-x11-server: tigervnc: heap-based buffer overflow privilege escalation vulnerability

Keywords: Security

Reported: 2024-10-08 13:44 UTC by OSIDB Bzimport

Status: NEW

Modified: 2025-08-04 16:33 UTC ([History](#))

Alias: CVE-2024-9632

CC List: 3 users ([show](#))

Deadline: 2024-10-29

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:

Blocks:


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

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:10090	0	None	None	None	2024-11-20 11:57:51 UTC
Red Hat Product Errata	RHSA-2024:8798	0	None	None	None	2024-11-04 08:14:15 UTC
Red Hat	RHSA-2024:9540	0	None	None	None	2024-11-13

Product Errata						14:32:43 UTC
Red Hat Product Errata	RHSA-2024:9579	0	None	None	None	2024-11-13 18:17:49 UTC
Red Hat Product Errata	RHSA-2024:9601	0	None	None	None	2024-11-13 19:14:52 UTC
Red Hat Product Errata	RHSA-2024:9690	0	None	None	None	2024-11-14 18:40:18 UTC
Red Hat Product Errata	RHSA-2024:9816	0	None	None	None	2024-11-18 01:32:41 UTC
Red Hat Product Errata	RHSA-2024:9818	0	None	None	None	2024-11-18 01:20:49 UTC
Red Hat Product Errata	RHSA-2024:9819	0	None	None	None	2024-11-18 01:32:05 UTC
Red Hat Product Errata	RHSA-2024:9820	0	None	None	None	2024-11-18 01:27:24 UTC
Red Hat Product Errata	RHSA-2024:9901	0	None	None	None	2024-11-18 19:20:19 UTC
Red Hat Product Errata	RHSA-2025:12751	0	None	None	None	2025-08-04 16:33:32 UTC
Red Hat Product Errata	RHSA-2025:7163	0	None	None	None	2025-05-13 10:14:07 UTC
Red Hat Product Errata	RHSA-2025:7165	0	None	None	None	2025-05-13 10:14:57 UTC
Red Hat Product Errata	RHSA-2025:7458	0	None	None	None	2025-05-13 15:54:59 UTC

OSIDB Bzimport  2024-10-08 13:44:52 UTC[Description](#)

The `_XkbSetCompatMap()` function attempts to resize the ``sym_interpret`` buffer. However, it didn't update its size properly. It updated ``num_si`` only, without ``size_si``:
<https://gitlab.freedesktop.org/xorg/xserver/-/blob/cdb4d5648a818a8e8ab282341be37109589229ab/xkb/xkb.c#L2998>

The exploit uses bitmap to achieve the arbitrary read and write. It leads to LPE for some distributions (xorg in debian xfce is run as root under specific display driver) and RCE for ssh x11 forwarding environment.

The exploit doesn't work if the OS installed on vmware and default virtualbox. It works on virtualbox with VBoxVGA graphic controller.

errata-xmlrpc 2024-11-04 08:14:14 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:8798 <https://access.redhat.com/errata/RHSA-2024:8798>

errata-xmlrpc 2024-11-13 14:32:42 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:9540 <https://access.redhat.com/errata/RHSA-2024:9540>

errata-xmlrpc 2024-11-13 18:17:48 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2024:9579 <https://access.redhat.com/errata/RHSA-2024:9579>

errata-xmlrpc 2024-11-13 19:14:51 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2024:9601 <https://access.redhat.com/errata/RHSA-2024:9601>

errata-xmlrpc 2024-11-14 18:40:16 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.8 Extended Update Support

Via RHSA-2024:9690 <https://access.redhat.com/errata/RHSA-2024:9690>

errata-xmlrpc 2024-11-18 01:20:48 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2024:9818 <https://access.redhat.com/errata/RHSA-2024:9818>

errata-xmlrpc 2024-11-18 01:27:24 UTC

[Comment 13](#)

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-2024:9820 <https://access.redhat.com/errata/RHSA-2024:9820>

errata-xmlrpc 2024-11-18 01:32:04 UTC

[Comment 14](#)

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 Update Services for SAP Solutions
Red Hat Enterprise Linux 8.4 Telecommunications Update Service

Via RHSA-2024:9819 <https://access.redhat.com/errata/RHSA-2024:9819>

errata-xmllrpc 2024-11-18 01:32:40 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2024:9816 <https://access.redhat.com/errata/RHSA-2024:9816>

errata-xmllrpc 2024-11-18 19:20:18 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2024:9901 <https://access.redhat.com/errata/RHSA-2024:9901>

errata-xmllrpc 2024-11-20 11:57:50 UTC

[Comment 17](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:10090 <https://access.redhat.com/errata/RHSA-2024:10090>

errata-xmllrpc 2025-05-13 10:14:06 UTC

[Comment 20](#)

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 10:14:56 UTC

[Comment 21](#)

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 15:54:57 UTC

[Comment 22](#)

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>

errata-xmlrpc 2025-08-04 16:33:31 UTC

[Comment 23](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 6 Extended Lifecycle Support - EXTENSION

Via RHSA-2025:12751 <https://access.redhat.com/errata/RHSA-2025:12751>

Note

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

