



Bug 2257691 (CVE-2023-6816) - CVE-2023-6816 xorg-x11-server: Heap buffer overflow in DeviceFocusEvent and ProcXQueryPointer

Keywords:

Reported: 2024-01-10 14:02 UTC by Patrick Del Bello

Status: NEW

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

Alias: CVE-2023-6816

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

Product: Security Response

Fixed In Version: xorg-server-21.1.11, xwayland-23.2.4

Component: vulnerability

Clone Of:

Version: unspecified

Environment:

Hardware: All

Last Closed:

OS: Linux

Embargoed:

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2258926](#) [2258927](#)

Blocks: [2256538](#)

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

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:0320	0	None	None	None	2024-01-22 13:43:33 UTC
Red Hat Product Errata	RHSA-2024:0557	0	None	None	None	2024-01-30 10:56:25 UTC
Red Hat Product Errata	RHSA-2024:0558	0	None	None	None	2024-01-30 11:00:00 UTC

Red Hat Product Errata	RHSA-2024:0597	0	None	None	None	2024-01-30 14:10:02 UTC
Red Hat Product Errata	RHSA-2024:0607	0	None	None	None	2024-01-30 14:53:45 UTC
Red Hat Product Errata	RHSA-2024:0614	0	None	None	None	2024-01-30 15:21:27 UTC
Red Hat Product Errata	RHSA-2024:0617	0	None	None	None	2024-01-31 07:07:38 UTC
Red Hat Product Errata	RHSA-2024:0621	0	None	None	None	2024-01-30 16:07:42 UTC
Red Hat Product Errata	RHSA-2024:0626	0	None	None	None	2024-01-31 08:31:21 UTC
Red Hat Product Errata	RHSA-2024:0629	0	None	None	None	2024-01-31 08:43:44 UTC
Red Hat Product Errata	RHSA-2024:2169	0	None	None	None	2024-04-30 09:43:34 UTC
Red Hat Product Errata	RHSA-2024:2170	0	None	None	None	2024-04-30 09:43:22 UTC
Red Hat Product Errata	RHSA-2024:2996	0	None	None	None	2024-05-22 09:32:59 UTC
Red Hat Product Errata	RHSA-2025:12751	0	None	None	None	2025-08-04 16:33:40 UTC

Patrick Del Bello 2024-01-10 14:02:10 UTC

[Description](#)

Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255 but the X.Org Server was only allocating space for the device's number of buttons, leading to a heap overflow if a bigger value

was used.

Sandipan Roy 2024-01-18 04:15:49 UTC

[Comment 3](#)

Created tigervnc tracking bugs for this issue:

Affects: fedora-all [[bug-2258927](#)]

Created xorg-x11-server tracking bugs for this issue:

Affects: fedora-all [[bug-2258926](#)]

errata-xmlrpc 2024-01-22 13:43:32 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2024:0320 <https://access.redhat.com/errata/RHSA-2024:0320>

errata-xmlrpc 2024-01-30 10:56:24 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:0557 <https://access.redhat.com/errata/RHSA-2024:0557>

errata-xmlrpc 2024-01-30 10:59:59 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 Update Services for SAP Solutions

Red Hat Enterprise Linux 8.4 Telecommunications Update Service

Via RHSA-2024:0558 <https://access.redhat.com/errata/RHSA-2024:0558>

errata-xmlrpc 2024-01-30 14:10:01 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.8 Extended Update Support

Via RHSA-2024:0597 <https://access.redhat.com/errata/RHSA-2024:0597>

errata-xmlrpc 2024-01-30 14:53:45 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:0607 <https://access.redhat.com/errata/RHSA-2024:0607>

errata-xmlrpc 2024-01-30 15:21:24 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Extended Update Support

Via RHSA-2024:0614 <https://access.redhat.com/errata/RHSA-2024:0614>

errata-xmlrpc 2024-01-30 16:07:41 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Extended Update Support

Via RHSA-2024:0621 <https://access.redhat.com/errata/RHSA-2024:0621>

errata-xmlrpc 2024-01-31 07:07:37 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support
Red Hat Enterprise Linux 8.2 Update Services for SAP
Solutions
Red Hat Enterprise Linux 8.2 Telecommunications Update
Service

Via RHSA-2024:0617 <https://access.redhat.com/errata/RHSA-2024:0617>

errata-xmlrpc 2024-01-31 08:31:20 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2024:0626 <https://access.redhat.com/errata/RHSA-2024:0626>

errata-xmlrpc 2024-01-31 08:43:43 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2024:0629 <https://access.redhat.com/errata/RHSA-2024:0629>

errata-xmlrpc 2024-04-30 09:43:21 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:2170 <https://access.redhat.com/errata/RHSA-2024:2170>

errata-xmlrpc 2024-04-30 09:43:33 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:2169 <https://access.redhat.com/errata/RHSA-2024:2169>

errata-xmlrpc 2024-05-22 09:32:58 UTC

[Comment 17](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:2996 <https://access.redhat.com/errata/RHSA-2024:2996>

errata-xmlrpc 2025-08-04 16:33:39 UTC

[Comment 18](#)

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.

