



Bug 2253291 (CVE-2023-6377) - CVE-2023-6377 xorg-x11-server: out-of-bounds memory reads/writes in XKB button actions

Keywords:

Reported: 2023-12-06 17:03 UTC by Robb Gatica

Status: NEW

Modified: 2025-08-18 11:16 UTC
([History](#))

Alias: CVE-2023-6377

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

Product: Security Response

Fixed In Version: xorg-server-21.1.10, xwayland-23.2.3

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: [2254291](#) [2254292](#)

Blocks: 2253250

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

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2023:7886	0	None	None	None	2023-12-20 13:22:19 UTC
Red Hat Product Errata	RHSA-2024:0006	0	None	None	None	2024-01-02 08:42:51 UTC
Red Hat Product Errata	RHSA-2024:0009	0	None	None	None	2024-01-02 08:25:28 UTC

Red Hat Product Errata	RHSA-2024:0010	0	None	None	None	2024-01-02 08:53:20 UTC
Red Hat Product Errata	RHSA-2024:0014	0	None	None	None	2024-01-02 08:54:13 UTC
Red Hat Product Errata	RHSA-2024:0015	0	None	None	None	2024-01-02 08:54:22 UTC
Red Hat Product Errata	RHSA-2024:0016	0	None	None	None	2024-01-02 08:54:30 UTC
Red Hat Product Errata	RHSA-2024:0017	0	None	None	None	2024-01-02 08:42:28 UTC
Red Hat Product Errata	RHSA-2024:0018	0	None	None	None	2024-01-02 08:55:39 UTC
Red Hat Product Errata	RHSA-2024:0020	0	None	None	None	2024-01-02 08:54:55 UTC
Red Hat Product Errata	RHSA-2024:2169	0	None	None	None	2024-04-30 09:43:23 UTC
Red Hat Product Errata	RHSA-2024:2170	0	None	None	None	2024-04-30 09:43:14 UTC
Red Hat Product Errata	RHSA-2024:2995	0	None	None	None	2024-05-22 09:32:38 UTC
Red Hat Product Errata	RHSA-2024:2996	0	None	None	None	2024-05-22 09:32:45 UTC
Red Hat Product Errata	RHSA-2025:13998	0	None	None	None	2025-08-18 11:16:02 UTC

Robb Gatica 2023-12-06 17:03:37 UTC

[Description](#)

CVE-2023-6377: X.Org server: Out-of-bounds memory write in XKB button actions

Introduced in: xorg-server-1.6.0 (2009)
Fixed in: xorg-server-21.1.10 and xwayland-23.2.3
Found by: Jan-Niklas Sohn working with Trend Micro Zero Day Initiative

A device has XKB button actions for each button on the device. When a logical device switch happens (e.g. moving from a touchpad to a mouse), the server re-calculates the information available on the respective master device (typically the Virtual Core Pointer). This re-calculation only allocated enough memory for a single XKB action rather instead of enough for the newly active physical device's number of button. As a result, querying or changing the XKB button actions results in out-of-bounds memory reads and writes.

This may lead to local privilege escalation if the server is run as root or remote code execution (e.g. x11 over ssh).

xorg-server-21.1.10 and xwayland-23.2.3 have been patched to fix this issue.

TEJ RATHI 2023-12-13 05:48:13 UTC

[Comment 4](#)

This CVE is public now:
<https://lists.x.org/archives/xorg-announce/2023-December/003435.html>

TEJ RATHI 2023-12-13 05:49:30 UTC

[Comment 5](#)

Upstream Fix:
<https://gitlab.freedesktop.org/xorg/xserver/-/commit/0c1a93d319558fe3ab2d94f51d174b4f93810afd>

Sandipan Roy 2023-12-13 06:11:50 UTC

[Comment 6](#)

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

Affects: fedora-all [[bug-2254291](#)]

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

Affects: fedora-all [[bug-2254292](#)]

errata-xmlrpc 2023-12-20 13:22:18 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2023:7886 <https://access.redhat.com/errata/RHSA-2023:7886>

errata-xmlrpc 2024-01-02 08:25:27 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2024:0009 <https://access.redhat.com/errata/RHSA-2024:0009>

errata-xmlrpc 2024-01-02 08:42:27 UTC

[Comment 9](#)

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-2024:0017 <https://access.redhat.com/errata/RHSA-2024:0017>

errata-xmlrpc 2024-01-02 08:42:50 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2024:0006 <https://access.redhat.com/errata/RHSA-2024:0006>

errata-xmlrpc 2024-01-02 08:53:19 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:0010 <https://access.redhat.com/errata/RHSA-2024:0010>

errata-xmlrpc 2024-01-02 08:54:12 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.8 Extended Update Support

Via RHSA-2024:0014 <https://access.redhat.com/errata/RHSA-2024:0014>

errata-xmlrpc 2024-01-02 08:54:21 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Extended Update Support

Via RHSA-2024:0015 <https://access.redhat.com/errata/RHSA-2024:0015>

errata-xmlrpc 2024-01-02 08:54:29 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-2024:0016 <https://access.redhat.com/errata/RHSA-2024:0016>

errata-xmlrpc 2024-01-02 08:54:54 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Extended Update Support

Via RHSA-2024:0020 <https://access.redhat.com/errata/RHSA-2024:0020>

errata-xmlrpc 2024-01-02 08:55:39 UTC

[Comment 16](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:0018 <https://access.redhat.com/errata/RHSA-2024:0018>

errata-xmlrpc 2024-04-30 09:43:13 UTC

[Comment 19](#)

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 09:43:22 UTC

[Comment 20](#)

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 09:32:36 UTC

[Comment 21](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:2995 <https://access.redhat.com/errata/RHSA-2024:2995>

errata-xmlrpc 2024-05-22 09:32:44 UTC

[Comment 22](#)

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 2025-08-18 11:16:00 UTC

[Comment 24](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 6 Extended Lifecycle Support -
EXTENSION

Via RHSA-2025:13998 <https://access.redhat.com/errata/RHSA-2025:13998>

Note

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

