Bug 2451106 (CVE-2026-33999) - CVE-2026-33999 xorg: xwayland: X.Org X server: Denial of Service via integer underflow in XKB compatibility map handling

Keywords: Security

Status: NEW

Alias: CVE-2026-33999

Product: Security Response

Component: vulnerability

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

Reported: 2026-03-25 06:29 UTC by OSIDB Bzimport

Modified: 2026-04-29 13:07 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:10739	0	None	None	None	2026-04-27 08:29:52 UTC
Red Hat Product Errata	RHSA-2026:11352	0	None	None	None	2026-04-28 11:21:02 UTC
Red Hat Product Errata	RHSA-2026:11369	0	None	None	None	2026-04-28 14:53:17 UTC

Red Hat Product Errata	RHSA-2026:11388	0	None	None	None	2026-04-28 17:58:05 UTC
Red Hat Product Errata	RHSA-2026:11656	0	None	None	None	2026-04-29 12:01:23 UTC
Red Hat Product Errata	RHSA-2026:11692	0	None	None	None	2026-04-29 13:07:52 UTC

OSIDB Bzimport 2026-03-25 06:29:42 UTC Description

```
Integer Underflow (Wraparound) vulnerability in the XKB
compatibility map handling of the X.Org X server. The issue
occurs in XkbSetCompatMap() when a previously truncated
“compat” buffer leaves unused space that is later reused
without correctly updating the count of valid entries. This
can cause internal size/index calculations to become
inconsistent and potentially underflow, resulting in a buffer
read overrun when subsequent XKB requests are processed. An
attacker with access to the X11 server (local or via remote
X11 forwarding/SSH tunneling) can trigger the flaw without
user interaction, leading to memory-safety violations and
potentially a crash or more severe impact depending on how
Xorg/Xwayland is deployed.
```

errata-xmlrpc 2026-04-27 08:29:51 UTC Comment 4

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:10739 https://access.redhat.com/errata/RHSA-
2026:10739
```

errata-xmlrpc 2026-04-28 11:20:59 UTC Comment 5

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2026:11352 https://access.redhat.com/errata/RHSA-
2026:11352
```

errata-xmlrpc 2026-04-28 14:53:16 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:11369 https://access.redhat.com/errata/RHSA-2026:11369

errata-xmlrpc 2026-04-28 17:58:04 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:11388 https://access.redhat.com/errata/RHSA-2026:11388

errata-xmlrpc 2026-04-29 12:01:21 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2026:11656 https://access.redhat.com/errata/RHSA-2026:11656

errata-xmlrpc 2026-04-29 13:07:51 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2026:11692 https://access.redhat.com/errata/RHSA-2026:11692

Note

You need to log in before you can comment on or make changes to this bug.