Bug 2337620 (CVE-2025-23367) - CVE-2025-23367 org.wildfly.core:wildfly-server: Wildfly improper RBAC permission

Keywords: Security

Status: NEW

Alias: CVE-2025-23367

Deadline: 2025-03-03

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2025-01-14 15:30 UTC by OSIDB Bzimport

Modified: 2026-04-01 08:28 UTC (History)

CC List: 42 users (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-2025:3465	0	None	None	None	2025-04-01 13:10:07 UTC
Red Hat Product Errata	RHSA-2025:3467	0	None	None	None	2025-04-01 13:06:55 UTC
Red Hat	RHSA-2025:3989	0	None	None	None	2025-04-17

Product Errata						14:31:30 UTC
Red Hat Product Errata	RHSA-2025:3990	0	None	None	None	2025-04-17 14:31:53 UTC
Red Hat Product Errata	RHSA-2025:3992	0	None	None	None	2025-04-17 14:38:15 UTC
Red Hat Product Errata	RHSA-2025:4548	0	None	None	None	2025-05-06 14:30:37 UTC
Red Hat Product Errata	RHSA-2025:4549	0	None	None	None	2025-05-06 14:31:00 UTC
Red Hat Product Errata	RHSA-2025:4550	0	None	None	None	2025-05-06 14:29:56 UTC
Red Hat Product Errata	RHSA-2025:4552	0	None	None	None	2025-05-06 14:28:12 UTC

OSIDB Bzimport 2025-01-14 15:30:59 UTC Description

When the authorization to control management operations is secured using the Role Based Access Control provider a user without the required privileges can suspend or resume the server.

A user with a Monitor or Auditor role is supposed to have only read access permissions and should not be able to suspend the server.

The vulnerability is caused by the Suspend and Resume handlers not performing authorization checks to validate whether the current user has the required permissions to proceed with the action.

When a server is suspended, the server will stop receiving user requests. The resume handle does the opposite; it will cause a suspended server to start accepting user requests.

Standalone server (Domain mode is not affected).
RBAC access control must be enabled with RBAC provider.
There is a user with a Monitor or Auditor role.

errata-xmlrpc 2025-04-01 13:06:52 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform

Via RHSA-2025:3467 https://access.redhat.com/errata/RHSA-2025:3467

errata-xmlrpc 2025-04-01 13:10:04 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.4 on RHEL 7
  Red Hat JBoss Enterprise Application Platform 7.4 for RHEL 8
  Red Hat JBoss Enterprise Application Platform 7.4 for RHEL 9

Via RHSA-2025:3465 https://access.redhat.com/errata/RHSA-2025:3465

errata-xmlrpc 2025-04-17 14:31:27 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8

Via RHSA-2025:3989 https://access.redhat.com/errata/RHSA-2025:3989

errata-xmlrpc 2025-04-17 14:31:50 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9

Via RHSA-2025:3990 https://access.redhat.com/errata/RHSA-2025:3990

errata-xmlrpc 2025-04-17 14:38:12 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform

Via RHSA-2025:3992 https://access.redhat.com/errata/RHSA-2025:3992

errata-xmlrpc 2025-05-06 14:28:07 UTC Comment 7

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform

Via RHSA-2025:4552 https://access.redhat.com/errata/RHSA-2025:4552

errata-xmlrpc 2025-05-06 14:29:52 UTC Comment 8

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7.4 for RHEL 9

Via RHSA-2025:4550 https://access.redhat.com/errata/RHSA-2025:4550

errata-xmlrpc 2025-05-06 14:30:34 UTC Comment 9

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7.4 on RHEL 7

Via RHSA-2025:4548 https://access.redhat.com/errata/RHSA-2025:4548

errata-xmlrpc 2025-05-06 14:30:56 UTC Comment 10

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7.4 for RHEL 8

Via RHSA-2025:4549 https://access.redhat.com/errata/RHSA-2025:4549

errata-xmlrpc 2025-10-23 22:29:46 UTC Comment 13

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7

Via RHSA-2025:4552 https://access.redhat.com/errata/RHSA-

2025:4552

Note

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