GitHub Advisory Database / GitHub Reviewed / CVE-2025-23367

WildFly improper RBAC permission

Moderate severity | GitHub Reviewed | Published on Jan 31, 2025 in **wildfly/wildfly-core** • Updated on Dec 8, 2025

Vulnerability details | Dependabot alerts 0

Package

org.wildfly.core:wildfly-server (Maven)

Affected versions	Patched versions
< 27.0.1.Final	27.0.1.Final
= 28.0.0.Beta1	28.0.0.Beta2

Description

A flaw was found in the Wildfly Server Role Based Access Control (RBAC) provider. When 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.

Impact

Standalone server (Domain mode is not affected) with use access control enabled with RBAC provider can be suspended or resumed by unauthorized users. 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.

Patches

Fixed in WildFly Core 27.0.1.Final

Workarounds

No workaround available

References

See also: https://issues.redhat.com/browse/WFCORE-7153

Acknowledgements

The WildFly project would like to thank Claudia Bartolini (TIM S.p.A), Marco Ventura (TIM S.p.A), and Massimiliano Brolli (TIM S.p.A) for reporting this issue. https://www.gruppotim.it/it/footer/red-team.html

References

- GHSA-qr6x-62gq-4ccp
- https://nvd.nist.gov/vuln/detail/CVE-2025-23367
- https://access.redhat.com/security/cve/CVE-2025-23367
- https://bugzilla.redhat.com/show_bug.cgi?id=2337620
- https://access.redhat.com/errata/RHSA-2025:3465
- https://access.redhat.com/errata/RHSA-2025:3467
- https://access.redhat.com/errata/RHSA-2025:3989
- https://access.redhat.com/errata/RHSA-2025:4548
- https://access.redhat.com/errata/RHSA-2025:4549
- https://access.redhat.com/errata/RHSA-2025:4550
- https://access.redhat.com/errata/RHSA-2025:4552
- https://access.redhat.com/errata/RHSA-2025:3990
- https://access.redhat.com/errata/RHSA-2025:3992

yersan published to wildfly/wildfly-core on Jan 31, 2025

Published to the GitHub Advisory Database on Jan 31, 2025

Reviewed on Jan 31, 2025

Last updated on Dec 8, 2025

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low

User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

EPSS score

0.199% (42nd percentile)

Weaknesses

▶ CWE-284

CVE ID

CVE-2025-23367

GHSA ID

GHSA-qr6x-62gq-4ccp

Source code

wildfly/wildfly-core

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.