Security Advisory WSO2-2025-4684/CVE-2025-12624

Published: 2026-01-26

Version: 1.0.0

Severity: Medium

CVSS Score: 6 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L) [https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L]

CVE IDs: CVE-2025-12624 [https://www.cve.org/CVERecord?id=CVE-2025-12624]

AFFECTED PRODUCTS

- WSO2 Identity Server: 5.2.0

OVERVIEW

Improper token invalidation after account lock.

DESCRIPTION

Due to not invalidating or revoking active access tokens upon account locking, users with locked accounts can continue using previously issued tokens to access protected resources. This behavior creates a security gap that allows unauthorized access until the tokens naturally expire.

IMPACT

The identified vulnerability could allow locked user accounts to continue accessing protected resources using existing valid tokens, resulting in unauthorized access and a potential violation of access control policies.

SOLUTION

Community Users (Open Source)

Migrate to the latest unaffected version of the respective WSO2 product(s).

Support Subscription Holders

Update your product to the specified update level, or to a higher update level, to mitigate the identified vulnerability.

> **Info**
>
> **WSO2 Support Subscription Holders may use WSO2 Updates [https://wso2.com/updates/] in order to apply the fix.**

Product Name	Product Version	Update Level
WSO2 Identity Server	5.2.0	35