



# Improper Token Invalidation in WSO2 Identity Server Allows Access After Account Lock

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-12624
<b>State</b>	PUBLISHED
<b>Assigner</b>	WSO2
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-16 11:16:26 UTC
<b>Updated</b>	2026-04-23 15:34:32 UTC
<b>Description</b>	Active access tokens are not revoked or invalidated when a user account is locked within WSO2 Identity Server. This failure

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000100000 probability, percentile 0.011370000 (date 2026-04-26)

**Problem Types:** CWE-613 | CWE-613 CWE-613: Insufficient Session Expiration

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	ed10eef1-636d-4f8e-9993-6890dfa878f8	Secondary	6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wso2	Identity Server	5.2.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WSO2	WSO2 Identity Server	unknown 5.2.0 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.2.0 5.2.0.35 custom	Not specified

### References

Reference	Source	Link
security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO...	ed10eef1-636d-4fbe-9993-6890dfa878f8	secu...
CVE Program record	CVE.ORG	www...
NVD vulnerability detail	NVD	nvd...

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Solutions

**CNA:** Follow the instructions given on <https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2025-4684/#solution>

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)