



Authorization Bypass via Adaptive Authentication in WSO2 Identity Server Allows Cross-Organization Account Takeover

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2025-9973 |
| State | PUBLISHED |
| Assigner | WSO2 |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-11 12:16:11 UTC |
| Updated | 2026-05-11 16:17:29 UTC |
| Description | Due to not validating the organization context when executing adaptive authentication flows, the WSO2 Identity Server allow |

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from ed10eef1-636d-4fbe-9993-6890dfa878f8

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

EPSS: 0.000220000 probability, percentile 0.063200000 (date 2026-05-12)

Problem Types: CWE-284 | CWE-863 | CWE-284 CWE-284 Improper Access Control | CWE-863 CWE-863 Incorrect Authorization

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | ed10eef1-636d-4fbe-9993-6890dfa878f8 | Secondary | 6.4 | MEDIUM | CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L |
| 3.1 | CNA | CVSS | 6.4 | MEDIUM | CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L |

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|---|---------------------------------|---------------|
| CNA | WSO2 | WSO2 Identity Server | affected 7.1.0 7.1.0.26 custom | Not specified |
| CNA | WSO2 | Conditional Authentication User And Roles Related Functions | affected 1.2.76 1.2.76.1 custom | Not specified |
| CNA | WSO2 | Conditional Authentication User And Roles Related Functions | unaffected 1.2.82 * 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/WSO2-2025-4530/#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

CVE.report and Source URL Uptime Status status.cve.report