Security Advisory WSO2-2025-4577/CVE-2025-10503

Published: 2026-01-26

Version: 1.0.0

Severity: Medium

CVSS Score: 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) [https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]

CVE IDs: CVE-2025-10503 [https://www.cve.org/CVERecord?id=CVE-2025-10503]

AFFECTED PRODUCTS

- WSO2 Identity Server: 7.1.0

OVERVIEW

Reflected Cross-Site Scripting (XSS) has been identified in the authentication endpoint.

DESCRIPTION

Due to improper output encoding, a Reflected Cross-Site Scripting (XSS) attack can be carried out by injecting a malicious payload through an unrestricted user input.

IMPACT

By leveraging the XSS attack, a malicious actor can make the browser get redirected to a malicious website, make changes in the UI of the web page, retrieve information from the browser, or cause harm otherwise. However, since all the session-related sensitive cookies are set with the httpOnly flag and protected, session hijacking or similar attacks would not be possible.

SOLUTION

Community Users (Open Source)

Apply the relevant fixes to your product using the public fix(es) provided below.

- https://github.com/wso2/identity-apps/pull/8295 [https://github.com/wso2/identity-apps/pull/8295]

If applying the fix or update is not feasible, 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	7.1.0	28