Security Advisory WSO2-2025-4251/CVE-2025-6024

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-2025-6024 [https://www.cve.org/CVERecord?id=CVE-2025-6024]

AFFECTED PRODUCTS

- WSO2 API Manager: 4.1.0, 4.0.0, 3.2.1, 3.2.0, 3.1.0
- WSO2 Identity Server: 5.11.0, 5.10.0

OVERVIEW

Reflected Cross Site Scripting (XSS) in the authentication endpoint.

DESCRIPTION

Due to lack of output encoding, an attacker can inject a malicious script into the authentication endpoint.

IMPACT

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

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 API Manager	4.1.0	238
WSO2 API Manager	4.0.0	375
WSO2 API Manager	3.2.1	74
WSO2 API Manager	3.2.0	455
WSO2 API Manager	3.1.0	351
WSO2 Identity Server	5.11.0	405
WSO2 Identity Server	5.10.0	360