

Security Advisory WSO2-2024-3391/CVE-2024-4867

Published: 2026-01-26

Version: 1.0.0

Severity: Medium

CVSS Score: 5.4 (CVSS:3.1/AV:N/AC:L/PR:L/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:L/UI:R/S:C/C:L/I:L/A:N>]

CVE IDs: [CVE-2024-4867](https://www.cve.org/CVERecord?id=CVE-2024-4867) [<https://www.cve.org/CVERecord?id=CVE-2024-4867>]

AFFECTED PRODUCTS

- WSO2 API Manager: 4.1.0, 4.0.0, 3.2.1, 3.2.0

OVERVIEW

Reflected Cross Site Scripting (XSS) vulnerabilities have been identified on the developer portal.

DESCRIPTION

Due to lack of encoding for untrusted user input the malicious actor may exploit the cross site scripting vulnerability on the developer portal.

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 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 | 187 |
| WSO2 API Manager | 4.0.0 | 293 |
| WSO2 API Manager | 3.2.1 | 32 |
| WSO2 API Manager | 3.2.0 | 408 |