Security Advisory WSO2-2024-3255/CVE-2024-2374

Published: 2026-01-26

Version: 1.0.0

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) [https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N]

CVE IDs: CVE-2024-2374 [https://www.cve.org/CVERecord?id=CVE-2024-2374]

AFFECTED PRODUCTS

- WSO2 API Manager: 4.3.0, 4.2.0, 4.1.0, 4.0.0, 3.2.0, 3.1.0
- WSO2 Identity Server as Key Manager: 5.10.0
- WSO2 Identity Server: 6.1.0, 6.0.0, 5.11.0, 5.10.0
- WSO2 Open Banking AM: 2.0.0
- WSO2 Open Banking IAM: 2.0.0

OVERVIEW

Potential XML External Entity Injection (XXE) vulnerabilities.

DESCRIPTION

Due to the improper usage of XML parser External Entity injection attacks can be exploited by a malicious actor.

IMPACT

By leveraging the vulnerability a malicious actor could read confidential files from the file system or access limited HTTP resources that are reachable (over HTTP GET requests) to the vulnerable product. The same vulnerability could be used to perform denial of service attacks by exhausting server resources.

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	4.3.0	57
WSO2 API Manager	4.2.0	144
WSO2 API Manager	4.1.0	206
WSO2 API Manager	4.0.0	280
WSO2 API Manager	3.2.0	368
WSO2 API Manager	3.1.0	278
WSO2 Identity Server	6.1.0	136
WSO2 Identity Server	6.0.0	179
WSO2 Identity Server	5.11.0	329
WSO2 Identity Server	5.10.0	300
WSO2 Identity Server as Key Manager	5.10.0	296
WSO2 Open Banking AM	2.0.0	328
WSO2 Open Banking IAM	2.0.0	348