Security Advisory WSO2-2024-3581/CVE-2024-8010

Published: 2026-01-26

Version: 1.0.0

Severity: Low

CVSS Score: 3.5 (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) [https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N]

CVE IDs: CVE-2024-8010 [https://www.cve.org/CVERecord?id=CVE-2024-8010]

AFFECTED PRODUCTS

- WSO2 API Manager: 4.3.0, 4.2.0, 4.1.0, 4.0.0, 3.2.1, 3.2.0

OVERVIEW

Potential XML external entity (XXE) injection vulnerabilities.

DESCRIPTION

Due to improper XML parser usage malicious actors may perform an XML external entity (XXE) injection attack by passing a malicious XML file through the publisher.

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.

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	39
WSO2 API Manager	4.2.0	127
WSO2 API Manager	4.1.0	171
WSO2 API Manager	4.0.0	310
WSO2 API Manager	4.0.0	319
WSO2 API Manager	3.2.1	27
WSO2 API Manager	3.2.0	397