Security Advisory WSO2-2025-3993/CVE-2025-2905

Published: 2025-05-05

Version: 1.0.0

Severity: Critical

CVSS Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)

AFFECTED PRODUCTS

- WSO2 API Manager 2.0.0 and earlier

OVERVIEW

An XML External Entity (XXE) vulnerability in the gateway component.

DESCRIPTION

The gateway component does not properly validate XML input when processing crafted URL paths. Specifically, user-supplied XML is parsed without applying sufficient restrictions, enabling XML External Entity (XXE) resolution.

IMPACT

A successful XXE attack could allow a remote, unauthenticated attacker to:

- **Read arbitrary files** from the server filesystem. The extent of this depends on the Java runtime environment:
    - On JDK 7 or early JDK 8, full file contents can be accessed.
    - On later versions of JDK 8 and newer, only the first line of a file may be exposed.
- **Perform denial-of-service (DoS) attacks**, which can render the affected service unavailable.

SOLUTION

No new fix will be released for this vulnerability as it has already been addressed in the patch provided for WSO2-2016-0151 [https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2016/WSO2-2016-0151/], which resolved a previously disclosed XSS vulnerability in the gateway component as well as this vulnerability.

If your deployment has already applied the fix for WSO2-2016-0151, no further action is required for this issue. However, if the earlier fix has not yet been applied, we strongly recommend doing so as it mitigates both the previously disclosed XSS and this newly identified XXE vulnerability.

> **Info**
>
> Although this vulnerability shares its fix with a previously disclosed Medium severity issue (XSS), the impact of the XXE vulnerability is Critical (CVSS 9.1). We are publishing this advisory to ensure all users are aware of its severity.

CREDITS

WSO2 thanks, **crnkovic** for responsibly reporting the identified issue and working with us as we addressed it.