مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in WSO2 API Manager

Tracking #:432317308

Date:26-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical XML External Entity (XXE) vulnerability (CVE-2025-2905) has been disclosed in the gateway component of WSO2 API Manager.

TECHNICAL DETAILS:

A critical XML External Entity (XXE) vulnerability (CVE-2025-2905) has been disclosed in the gateway component of WSO2 API Manager versions 2.0.0 and below. This vulnerability arises from improper validation of XML input when processing crafted URL paths, allowing malicious actors to exploit the application remotely without authentication.

A successful exploit could allow attackers to read arbitrary files on the server filesystem or perform Denial-of-Service (DoS) attacks, depending on the configuration of the underlying Java runtime environment. Notably, the issue has already been resolved in the fix released for WSO2-2016-0151, which also addressed an unrelated XSS vulnerability.

Organizations using WSO2 API Manager versions prior to 2.0.0 and who have not applied the 2016 patch remain vulnerable to this high-impact issue.

Technical Details:

- Vulnerability Type: XML External Entity (XXE) Injection
- CVE Identifier: CVE-2025-2905
- Component Affected: WSO2 API Manager - Gateway Component
- Attack Vector: Remote / Unauthenticated
- Conditions:
  - **XML input sent via specially crafted URL paths**
  - **Improper restriction on XML entity resolution**

Impact:

- **Information Disclosure:**
  Attackers can read files from the server filesystem. The extent varies:
  - **JDK 7 / Early JDK 8:** Full file content exposure
  - **Later JDK 8+ Versions:** Partial disclosure (e.g., first line only)
- **Denial-of-Service (DoS):**
  Malicious payloads can cause the gateway component to crash or become unresponsive.

RECOMMENDATIONS:

- Patch Deployment: Organizations who have not applied the patch for WSO2-2016-0151, do so immediately. This patch mitigates both the original XSS vulnerability and this critical XXE issue.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2025/WSO2-2025-3993/