مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in WSO2 Products

Tracking #:432316493

Date:11-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical authentication and authorization vulnerabilities identified in WSO2 API Manager and Identity Server Products.

TECHNICAL DETAILS:

WSO2 has issued a security advisory for multiple critical vulnerabilities affecting its API Manager, Identity Server, and related products. These vulnerabilities could allow an attacker to bypass authentication mechanisms or reset user passwords, potentially compromising sensitive accounts, including administrators.

Two critical vulnerabilities have been disclosed in WSO2 API Manager and Identity Server products:

1. **Broken Authentication Vulnerability in REST API Endpoints**:
    - **Severity**: Critical (CVSS: 9.4)
    - Affected versions: WSO2 API Manager 4.2.0.
    - Description: A broken authentication vulnerability allows attackers to manipulate REST API paths and bypass authentication checks, enabling impersonation of other users, including admins. The exploitation of this flaw could lead to unauthorized access and control of critical resources.
2. **Weakness in SOAP Admin Services**:
    - **Severity**: Critical (CVSS: 9.8) when publicly exposed, or High (CVSS: 8.8) when restricted to trusted networks.
    - Affected versions: Multiple versions of WSO2 API Manager, Identity Server, and Open Banking products.
    - Description: Exposed SOAP Admin Services via the "/services" context path can be exploited to reset passwords and take control of user accounts, including those with elevated privileges. If these services are publicly exposed, attackers can remotely hijack accounts, including administrative accounts.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to download the latest patches and versions from WSO2's official update channels.

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/2024/WSO2-2023-2803/
- https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2024/WSO2-2024-3561/