مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in IBM webMethods Integration

Tracking #:432316253

Date:10-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in IBM webMethods Integration Server that could be exploited to gain unauthorized access, escalate privileges, and potentially compromise the entire system.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-45076 (CVSS v3 Score: 9.9 - CRITICAL):** This vulnerability allows an authenticated user to upload and execute arbitrary files, potentially leading to remote code execution on the underlying operating system.
- **CVE-2024-45075 (CVSS v3 Score: 8.8 - HIGH):** This vulnerability allows an authenticated user to escalate their privileges to administrator level by exploiting missing authentication controls in scheduler tasks.
- **CVE-2024-45074 (CVSS v3 Score: 6.5 - MEDIUM):** This vulnerability allows an authenticated user to perform directory traversal attacks on the server. This could allow an attacker to access sensitive information stored on the system.

Affected Versions:

- IBM webMethods Integration Server version 10.15

Remediation/Fixes:

- Download and install Corefix 14 of Integration Server using Update Manager.
- Refer to the instructions **here** for applying the fix

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://www.ibm.com/support/pages/node/7167245