مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authentication Bypass Vulnerability in IBM Maximo Application Suite

Tracking #:432317872

Date:29-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has disclosed a critical authentication bypass vulnerability (CVE-2025-36386) affecting the IBM Maximo Manage component in the IBM Maximo Application Suite (MAS) when integrated with standalone Cognos Analytics via the MXCSP integration mechanism.

TECHNICAL DETAILS:

A remote, unauthenticated attacker could exploit this flaw to bypass authentication controls and gain unauthorized access to Cognos Analytics, potentially exposing sensitive operational and business data. The vulnerability requires no user interaction and can be exploited over the network, making it a high-priority target for exploitation.

There are currently no workarounds or mitigations, and IBM has issued critical patch updates via Fix Central. Organizations using affected versions should upgrade immediately to mitigate risk.

Vulnerability Details

- CVE ID: CVE-2025-36386
- CVSS v3.1 Base Score: 9.8 (Critical)
- Description: A flaw in the IBM Maximo Manage application's authentication mechanism allows attackers to bypass authentication when integrating MAS with standalone Cognos Analytics using MXCSP. This could lead to full unauthorized access to sensitive data or system functions.
- CWE Reference: CWE-305 – Authentication Bypass by Primary Weakness

Affected Products and Versions

Product	Affected Versions
IBM Maximo Application Suite – Manage Component (MAS 9.0.x)	MAS 9.0.0 to 9.0.15 – Manage 9.0.0 to 9.0.17
IBM Maximo Application Suite – Manage Component (MAS 9.1.x)	MAS 9.1.0 to 9.1.4 – Manage 9.1.0 to 9.1.4

Fixed Version:

- IBM Maximo Application Suite 9.0
- IBM Maximo Application Suite 9.1

RECOMMENDATIONS:

- Immediate Patch Deployment: Upgrade to the latest available fix packs as provided by IBM via Fix Central.

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/7249416