مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authentication Bypass Vulnerability in IBM API Connect
Tracking #:432318191
Date:30-12-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has disclosed a critical authentication bypass vulnerability affecting IBM API Connect.

TECHNICAL DETAILS:

IBM has disclosed a critical authentication bypass vulnerability affecting IBM API Connect, tracked as CVE-2025-13915.The flaw allows unauthenticated remote attackers to bypass login controls entirely and gain unauthorized access to affected systems.With a CVSS v3.1 base score of 9.8 (Critical), this vulnerability poses a severe risk to enterprise API infrastructures, potentially leading to data exposure, service manipulation, and further compromise of backend systems.
IBM has released interim fixes (iFixes) for all affected versions and strongly urges immediate remediation**.**

Vulnerability Details
- CVE-2025-13915
- CVSS Source: IBM
- CVSS Base score: 9.8,Critical
- CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Products
- IBM API Connect V10.0.8-10.0.8.0 – 10.0.8.5
- IBM API Connect V10.0-10.0.11.0

Remediation and Fixes
- IBM has released official interim fixes (iFixes) for all impacted versions.

Workarounds & Temporary Mitigations
   For organizations unable to immediately apply the fix, IBM recommends the following temporary mitigation:
- Disable self-service sign-up on the Developer Portal, if enabled

RECOMMENDATIONS:

- Identify all IBM API Connect deployments within environment and apply the appropriate iFix immediately based on the deployed version.

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/7255149