

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in IBM Watsonx Orchestrate Cartridge
Tracking #:432317662
Date:02-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Watsonx Orchestrate cartridge for IBM Cloud Pak for Data that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

IBM has disclosed a high-severity vulnerability in the Watsonx Orchestrate Cartridge for IBM Cloud Pak for Data, tracked as CVE-2025-0165. The flaw enables blind SQL injection attacks, allowing authenticated attackers to execute crafted SQL statements on the back-end database. This vulnerability could result in unauthorized data access, manipulation, or deletion, posing significant confidentiality, integrity, and availability risks.

Vulnerability Details

- **CVE-2025-0165**
- **CVSS Score 7.6 High**
- Blind SQL injection in IBM Watsonx Orchestrate Cartridge allows attackers to view, modify, or delete data.
- **Impact:**
 - **Confidentiality:** Exposure of sensitive data (e.g., credentials, proprietary information)
 - **Integrity:** Modification or insertion of unauthorized records
 - **Availability:** Deletion or corruption of critical database tables, leading to service disruption
- **Attack Vector:** Authenticated user with access to vulnerable workflows can inject SQL through unsanitized input fields.

Affected Versions

- 4.8.4 through 4.8.5
- 5.0.0 through 5.2

Fixed Versions:

- IBM Watsonx Orchestrate Cartridge version 5.2.0.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by IBM.

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/7243596>