مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in IBM Db2

Tracking #:432319232

Date:02-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has released security updates to address multiple vulnerabilities affecting IBM Db2 for Linux, UNIX, and Windows (LUW).

TECHNICAL DETAILS:

IBM has released security updates to address multiple vulnerabilities affecting IBM Db2 for Linux, UNIX, and Windows (LUW). The most severe issue, CVE-2026-10109, is a Critical pre-authentication Remote Code Execution (RCE) vulnerability with a CVSS v3.1 score of 9.8.
The vulnerability exists in the Distributed Relational Database Architecture (DRDA) connection handshake process and can allow an unauthenticated remote attacker to execute arbitrary code on a vulnerable Db2 server without requiring valid credentials. Given that Db2 is widely deployed to support mission-critical enterprise applications and databases, successful exploitation could lead to complete system compromise, data theft, service disruption, or lateral movement within enterprise environments. At the time of publication, IBM has not reported active exploitation or released technical exploit details. Organizations are strongly advised to apply the available security updates immediately and restrict network exposure until remediation is completed.

Vulnerability Details

1. CVE-2026-10109 – Pre-Authentication Remote Code Execution (Critical)
   - CVE ID: CVE-2026-10109
   - Severity: Critical
   - CVSS v3.1 Score: 9.8
   - Vulnerability Type: Remote Code Execution (RCE)
   - CWE: CWE-94 – Improper Control of Generation of Code ('Code Injection')
2. **CVE-2025-36372 – Information Disclosure**
   - **Severity:** Medium
   - Authenticated information disclosure vulnerability.
   - An authenticated user may gain unauthorized access to sensitive information stored in Db2 monitoring tables.
3. **CVE-2026-11906 – Denial of Service (DoS)**
   - **Severity:** Medium
   - Authenticated denial-of-service vulnerability.
   - A specially crafted XMLTable query against a federated server can cause the Db2 server to crash.

Affected Products:

- Db2 11.5.0 through 11.5.9
- Db2 12.1.0 through 12.1.4

Affected platforms include:

- Linux
- UNIX
- Windows

Fixed Versions:

- Db2 11.5: Special Build #84653 or later
- Db2 12.1: Special Build #86230 or later

RECOMMENDATIONS:

Immediate Actions:

- Apply IBM security updates as soon as possible.
- Validate successful installation of the updated builds.

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/7277424