

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – IBM TXSeries for Multiplatforms

Tracking #:432316921

Date:03-03-2025

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 IBM has released a security bulletin addressing a vulnerability in the Apache Derby package shipped with IBM TXSeries for Multiplatforms. This vulnerability could allow a remote attacker to bypass security restrictions due to an LDAP injection vulnerability in the authenticator.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2022-46337
- **CVSS Base Score:** 9.1 **Critical**
- Apache Derby could allow a remote attacker to bypass security restrictions due to an LDAP injection vulnerability in the authenticator. By sending a specially crafted request, an attacker could exploit this vulnerability to access and modify sensitive data and execute sensitive database functions and procedures.

Affected Versions:

- IBM TXSeries for Multiplatforms versions 8.1, 8.2, 9.1, and 10.1

Note: Refer to the IBM security bulletin for details on fixed versions and additional information

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/7184192>