مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in IBM Cognos Analytics

Tracking #:432316658

Date:23-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in IBM Cognos Analytics, which could be exploited to steal data, disrupt operations, and compromise system integrity.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-51466**
  - CVSS Score 9.0 Critical
  - An Expression Language (EL) Injection vulnerability that allows remote attackers to execute specially crafted EL statements, potentially exposing sensitive information, consuming memory resources, and causing server crashes.
  - This vulnerability can be exploited remotely without authentication, potentially leading to sensitive data exposure, resource consumption, and server crashes
- **CVE-2024-40695**
  - CVSS Score 8.0 High
  - A Malicious File Upload vulnerability that enables privileged users to upload and execute malicious files due to insufficient file validation in the web interface.
  - This vulnerability can allow privileged users to upload malicious executable files, execute them within the system, and potentially use them as vectors for further attacks.

Affected Versions:

- IBM Cognos Analytics versions 12.0.0 through 12.0.4
- IBM Cognos Analytics versions 11.2.0 through 11.2.4 FP4

Fixed Versions:

- IBM Cognos Analytics 12.0.4 Interim Fix 1
- IBM Cognos Analytics 11.2.4 FP5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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/7179496