مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Rockwell Automation FactoryTalk

Tracking #:432316816

Date:03-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Rockwell Automation has disclosed multiple critical vulnerabilities affecting FactoryTalk AssetCentre. These flaws could allow attackers to compromise industrial control systems (ICS), potentially leading to data breaches, system disruption, and unauthorized control.

TECHNICAL DETAILS:

Rockwell Automation has issued a security advisory addressing multiple critical vulnerabilities in its FactoryTalk AssetCentre software. These flaws, tracked as CVE-2025-0477, CVE-2025-0497, and CVE-2025-0498, pose severe risks to industrial control systems (ICS) by allowing attackers to extract credentials, expose sensitive data, and impersonate users.

Vulnerability Details:

- **CVE-2025-0477 – Weak Encryption of Stored Credentials (CVSS 9.8 – Critical)**
  - This encryption vulnerability could allow a threat actor to extract passwords belonging to other users of the application.
- **CVE-2025-0497 – Credential Exposure in Configuration Files (CVSS 7.0 – High)**
  - Credentials are stored in configuration files of various software packages, including EventLogAttachmentExtractor and ArchiveExtractor. Attackers with access to these files could retrieve and misuse stored credentials, posing a risk to operational integrity.
- **CVE-2025-0498 – Insecure Storage of Security Tokens (CVSS 7.8 – High)**
  - Attackers can steal FactoryTalk Security user tokens, enabling them to impersonate legitimate users.

Affected Versions:

- FactoryTalk AssetCentre prior to v15.00.01.

Fixed Versions:

- FactoryTalk AssetCentre v15.00.01 or later

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.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1721.html