مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Rockwell Automation FactoryTalk Systems

Tracking #:432317281

Date:19-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Rockwell Automation has disclosed a critical vulnerability affecting its FactoryTalk Historian-ThingWorx Connector, stemming from a third-party component—Apache log4net.

TECHNICAL DETAILS:

Rockwell Automation has disclosed a critical vulnerability affecting its FactoryTalk Historian-ThingWorx Connector, stemming from a third-party component—Apache log4net.

Vulnerability Details

- CVE ID: CVE-2018-1285
- Severity: Critical (CVSS 9.8)
- Component: Apache log4net (logging library)
- Vulnerability Type: XML External Entity (XXE) Injection
- Attack Vector: Local or remote manipulation of configuration files
- Root Cause: Older log4net versions do not securely disable external XML entity resolution, allowing crafted configuration files to exploit system resources or disclose sensitive data.
- Affected Product: FactoryTalk Historian-ThingWorx Connector (95057C-FTHTWXCT11) ≤ v4.02.00
- Fixed Version:v5.00.00 and later

RECOMMENDATIONS:

- Update the FactoryTalk Historian-ThingWorx Connector to fixed version or later.

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.SD1728.html