



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in Rockwell Automation Products

Tracking #:432316290

Date:17-09-2024

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 critical vulnerabilities in Rockwell Automation FactoryTalk software products that could be exploited to gain unauthorized access and execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-45823: Authentication Bypass in FactoryTalk Batch View**
 - **Severity:** **Critical** (CVSSv4 score of 9.2)
 - **Description:** The vulnerability exists due to shared secrets across accounts, potentially allowing a threat actor to impersonate a user with additional information.
 - **Impact:** Unauthorized access to sensitive systems and data.
 - **Affected Versions:** FactoryTalk Batch View 2.01.00
- **CVE-2024-45824: Remote Code Execution in FactoryTalk View Site Edition**
 - **Severity:** **Critical** (CVSSv4 score of 9.2)
 - **Description:** The vulnerability occurs when chained with Path Traversal, Command Injection, and XSS Vulnerabilities and allows for full unauthenticated remote code execution.
 - **Impact:** Remote code execution without authentication, potentially leading to system compromise.
 - **Affected Versions:** FactoryTalk View Site Edition 12.0, 13.0, and 14.0

Fixed Versions:

- **FactoryTalk Batch View:** Upgrade to version 3.00.00 or later.
- **FactoryTalk View Site Edition:** Apply the patches available at the [link](#) provided by Rockwell Automation.

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.SD%201698.html>
- <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1696.html>