مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE & DoS Vulnerabilities in Rockwell Automation Devices

Tracking #:432316017

Date:03-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two vulnerabilities in Rockwell Automation PanelView Plus devices that can lead to remote code execution and Denial-of-Service.

TECHNICAL DETAILS:

Two vulnerabilities in Rockwell Automation's PanelView Plus devices that could allow remote code execution (RCE) and denial-of-service (DoS) attacks by unauthenticated attackers. The Remote Code Execution (RCE) vulnerability, identified as CVE-2023-2071 with a CVSS score of 9.8, involves the exploitation of two custom classes within the device. Attackers can abuse these classes to upload and execute a malicious DLL, effectively gaining remote control of the device.

The DoS vulnerability, labeled CVE-2023-29464 with a CVSS score of 8.2, exploits the same custom class to send a crafted buffer that the device cannot handle, leading to a system crash.

- **CVE-2023-2071**-CVSS Score 9.8-Remote code execution (RCE)
- **CVE-2023-29464**-CVSS Score 8.2-DoS via out-of-bounds read

Affected Products:

- FactoryTalk View Machine Edition: v13.0
- FactoryTalk View Machine Edition: v12.0 and prior
- FactoryTalk® Linx v6.20

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to corrected firmware revisions 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.PN1645%20.html