مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Rockwell Automation Products

Tracking #:432315773

Date:19-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in Rockwell Automation products that could allow an attacker to cause a denial-of-service (DoS) condition.

TECHNICAL DETAILS:

A vulnerability has been identified in Rockwell Automation's ControlLogix 5580, GuardLogix 5580, CompactLogix 5380, and 1756-EN4TR products that could allow an attacker to cause a denial-of-service (DoS) condition. A specifically crafted malformed fragmented packet could trigger a major nonrecoverable fault (MNRF) on the affected devices. This could result in a loss of view and/or control of connected devices.

Vulnerability Details

CVE ID: CVE-2024-3493
CVSS 4.0 Score: Base Score 9.2
Description: A specific malformed fragmented packet type can cause a major nonrecoverable fault (MNRF) on Rockwell Automation's ControlLogix 5580, Guard Logix 5580, CompactLogix 5380, and 1756-EN4TR products.

Affected Products:

- Rockwell Automation ControlLogix 5580 (version V35.011)
- Rockwell Automation GuardLogix 5580 (version V35.011)
- Rockwell Automation CompactLogix 5380 (version V35.011)
- Rockwell Automation 1756-EN4TR (version V5.001)

Mitigation:

- ControlLogix 5580: V35.013 or V36.011
- GuardLogix 5580: V35.013 or V36.011
- CompactLogix 5380: V35.013 or V36.011
- 1756-EN4TR: V6.001

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the patches released for affected products

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/support/advisory.SD1666.html