مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Rockwell Automation ThinManager

Tracking #:432316475
Date:06-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Rockwell Automation ThinManager that could be exploited to gain unauthorized access to sensitive data or cause denial-of-service conditions on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-10386**
  - **CVSS Score:** 9.8 (Critical)
  - An authentication vulnerability exists in the affected product. This vulnerability allows threat actors with network access to send crafted messages that could potentially manipulate the database of affected systems
- **CVE-2024-10387**
  - **CVSS Score:** 8.7 (High)
  - A Denial-of-Service (DoS) vulnerability exists in the affected product. This vulnerability could allow a malicious actor with network access to send specially crafted messages to the device, potentially causing the device to become unresponsive or crash.

Affected Product	Affected Versions	Fixed Versions
ThinManager	11.2.0-11.2.9 12.0.0-12.0.7 12.1.0-12.1.8 13.0.0-13.0.5 13.1.0-13.1.3 13.2.0-13.2.2 14.0.0	11.2.10 12.0.8 12.1.9 13.0.6 13.1.4 13.2.3 14.0.1

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.SD1708.html