مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Rockwell Automation ThinManager

Tracking #:432317159

Date:02-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Rockwell Automation has disclosed two high-severity vulnerabilities in ThinManager, its centralized management platform for industrial thin clients.

TECHNICAL DETAILS:

Rockwell Automation has disclosed two high-severity vulnerabilities in ThinManager, its centralized management platform for industrial thin clients. These flaws could allow attackers to escalate local privileges or crash systems via denial-of-service (DoS) attacks.

Vulnerability Details:

1. **CVE-2025-3617 – Local Privilege Escalation**
   - **Description:** A vulnerability exists where ThinManager improperly deletes files in a temporary directory during startup. This action causes file permission inheritance from the parent directory, possibly granting higher privileges to unauthorized users.
   - **Impact:** Local attackers with limited privileges may gain administrative access.
   - **CVSS v4.0:** 8.5 (High)
   - **CWE:** 276 – Incorrect Default Permissions
   - **Affected Versions:** 14.0.0 and 14.0.1
   - **Fixed In:** v14.0.2 and later

2. **CVE-2025-3618 – Denial of Service (DoS)**
   - **Description:** ThinManager fails to properly handle memory allocation when processing Type 18 messages. This flaw could lead to a **crash** or **service unavailability**.
   - **Impact:** Remote or local unauthenticated attackers can trigger a **denial-of-service**, affecting system reliability.
   - **CVSS v4.0:** 8.7 (High)
   - **CWE:** 119 – Improper Restriction of Operations within the Bounds of a Memory Buffer
   - **Affected Versions:** v14.0.1 and earlier
   - **Fixed in:** v11.2.11, 12.0.9, 12.1.10, 13.0.7, 13.1.5, 13.2.4, 14.0.2 and later

RECOMMENDATIONS:

- Update ThinManager to fixed version and enforce least privilege access on all users interacting with ThinManager.

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.SD1727.html