مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

# Security Updates – Rockwell Automation's ThinManager

Tracking #:432316191

Date:28-08-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Rockwell Automation's released security updates to address multiple vulnerabilities in ThinManager ThinServer software.

## TECHNICAL DETAILS:

**Vulnerability Details**:

- **CVE-2024-7988** -(CVSS v3.1- 9.8,Critical): A remote code execution vulnerability exists in the affected products that allows a threat actor to execute arbitrary code with System privileges. This vulnerability exists due to the lack of proper data input validation, which allows files to be overwritten.
- **CVE-2024-7987**-(CVSS v3.1-7.8) - A remote code execution vulnerability exists in the affected products that allows a threat actor to execute arbitrary code with System privileges. To exploit this vulnerability and a threat actor must abuse the ThinServer service by creating a junction and use it to upload arbitrary files.
- **CVE-2024-7986**-(CVSS v3.1-5.5): This vulnerability enables threat actors to disclose sensitive information by abusing the ThinServer service to read arbitrary files.

**Affected Products and Fixed Versions:**

| Impacted Product | Impacted Versions | Fixed Versions |
|---|---|---|
| ThinManager ThinServer | 11.1.0-11.1.7<br>11.2.0-11.2.8<br>12.0.0-12.0.6<br>12.1.0-12.1.7<br>13.0.0-13.0.4<br>13.1.0-13.1.2<br>13.2.0-13.2.1 | 11.1.8<br>11.2.9<br>12.0.7<br>12.1.8<br>13.0.5<br>13.1.3<br>13.2.2 |

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Rockwell Automation.

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.SD1692.html