مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in SolarWinds ARM

Tracking #:432316277

Date:16-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SolarWinds released security advisory to address two vulnerabilities affecting their Access Rights Manager (ARM) software.

TECHNICAL DETAILS:

SolarWinds has disclosed two vulnerabilities affecting their Access Rights Manager (ARM) software. The newly identified vulnerabilities, CVE-2024-28990 and CVE-2024-28991, have the potential to compromise the security of networks utilizing ARM, with impacts ranging from unauthorized access to remote code execution.

1. **CVE-2024-28991** (CVSS 9.0,Critical): Deserialization of Untrusted Data Remote Code Execution.
    - An authenticated attacker could exploit this flaw to execute malicious code on the targeted system, potentially leading to complete control over the ARM application and access to sensitive data.

2. **CVE-2024-28990** (CVSS 6.3): Hardcoded Credentials Authentication Bypass
    - Attackers could potentially gain unauthorized access to the RabbitMQ management console, a key component of the ARM system

➢ **Fixed Versions:** ARM version 2024.3.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update SolarWinds ARM to the fixed version 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://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3-1_release_notes.htm