



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- SolarWinds Access Rights Manager Critical Vulnerability

Tracking #:432315884

Date:23-05-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in SolarWinds Access Rights Manager (ARM). These vulnerabilities could allow attackers to gain unauthorized access to systems and potentially execute malicious code.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-28075 (Critical, CVSS Score: 9.0):** SolarWinds ARM Deserialization of Untrusted Data Remote Code Execution Vulnerability.
 - This vulnerability allows an authenticated attacker to abuse SolarWinds services and execute arbitrary code on the system.
- **CVE-2024-23473 (High, CVSS Score: 8.6):** SolarWinds Access Rights Manager (ARM) Hard-Coded Credentials Authentication Bypass Vulnerability.
 - This vulnerability allows unauthorized access to the SolarWinds ARM RabbitMQ management console by exploiting hard-coded credentials.
- A successful exploit of this vulnerability could grant attackers unauthorized access to sensitive information or complete control of affected systems.

Affected Versions:

- SolarWinds ARM 2023.2.3 and prior versions

Fixed Versions:

- SolarWinds ARM 2023.2.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version released by SolarWinds.

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.solarwinds.com/trust-center/security-advisories/cve-2024-28075>
- <https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23473>