



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – SOLARWINDS ARM

Tracking #:432316065

Date:18-07-2024

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 that SOLARWINDS released security updates to address multiple critical vulnerabilities in its Access Rights Manager (ARM) tool.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-23475** | Severity: **9.6 – Critical** | Directory Traversal and Information Disclosure Vulnerability
 - This vulnerability allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information.
- **CVE-2024-23469** | Severity: **9.6 – Critical** | Dangerous Method Remote Code Execution Vulnerability
 - This vulnerability allows an unauthenticated user to perform the actions with SYSTEM privileges.
- **CVE-2024-23472** | Severity: **9.6 – Critical** | Directory Traversal Arbitrary File Deletion and Information Disclosure Vulnerability
 - This vulnerability allows an authenticated user to arbitrary read and delete files in ARM.
- **CVE-2024-23466** | Severity: **9.6 – Critical** | Directory Traversal Remote Code Execution Vulnerability
 - If exploited, this vulnerability allows an unauthenticated user to perform the actions with SYSTEM privileges.
- **CVE-2024-23467** | Severity: **9.6 – Critical** | Directory Traversal Remote Code Execution Vulnerability
 - This vulnerability allows an unauthenticated user to perform remote code execution.
- **CVE-2024-28074** | Severity: **9.6 – Critical** | Internal Deserialization Remote Code Execution Vulnerability
 - This vulnerability allows an unauthenticated user to perform remote code execution.
- **CVE-2024-23471** | Severity: **9.6 – Critical** | CreateFile Directory Traversal Remote Code Execution Vulnerability
 - This vulnerability allows an authenticated user to abuse a SolarWinds service resulting in remote code execution.
- **CVE-2024-23470** | Severity: **9.6 – Critical** | UserScriptHumster Exposed Dangerous Method Remote Command Execution Vulnerability
 - This vulnerability allows an unauthenticated user to run commands and executables.

Fixed versions:

- Access Rights Manager 2024.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm