



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**High Severity Vulnerability in Schneider Electric Product**

Tracking #:432316142

Date:13-08-2024

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 Schneider Electric revealed a high severity vulnerability in its product; Accutech Manager.

## TECHNICAL DETAILS:

The Accutech Manager software is the configuration and monitoring application for Accutech Wireless sensor devices.

### Vulnerability Details:

- **CVE-2024-6918** | Base score: 7.5 | High | Buffer Copy without Checking Size of Input
  - The vulnerability may risk remote attacks from an unauthenticated user, which could result in resource exhaustion and loss of availability of the software.

### Affected Versions:

- Accutech Manager Versions prior to 2.10.0

### Fixed Versions:

- Accutech Manager Version 2.10.0

## RECOMMENDATIONS:

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

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://download.schneider-electric.com/files?p\\_Doc\\_Ref=SEVD-2024-226-01&p\\_enDocType=Security+and+Safety+Notice&p\\_File\\_Name=SEVD-2024-226-01.pdf](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-226-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-226-01.pdf)