مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Schneider Electric Products

Tracking #:432316613

Date:10-12-2024

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 INTELLGIENCE 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 Schneider Electric products that could potentially lead to severe security compromises, including denial of service, unauthorized access, and control of affected devices.

TECHNICAL DETAILS:

Vulnerabilities Details:
CVE-2024-11737: Critical Vulnerability in Modicon Controllers

- **CVSS v3.1 Base Score: 9.8 (Critical)**
- An Improper Input Validation vulnerability exists in Schneider Electric's Modicon Controllers M241, M251, M258, and LMC058. These Programmable Logic Controllers (PLCs) are designed for performance-demanding applications.
- This vulnerability could lead to a denial of service and compromise the confidentiality and integrity of the controller when an unauthenticated, crafted Modbus packet is sent to the device.
- **Affected Products:**
  - Modicon Controllers M241
  - Modicon Controllers M251
  - Modicon Controllers M258
  - Modicon Controllers LMC058

CVE-2024-11999: High-Severity Vulnerability in Harmony and Pro-face HMI Panels

- **CVSS v3.1 Base Score: 8.8 (High)**
- A Use of Unmaintained Third-Party Components vulnerability exists in Schneider Electric's Harmony HMI Panels and Pro-face HMI Panels. These panels are critical automation components managing vital machine features, including visualization, control, supervision, diagnostics, monitoring, and data logging.
- This vulnerability could allow an authenticated user to install malicious code into the HMI product, potentially leading to complete control of the device.
- **Affected Products:**
  - Harmony (Formerly Magelis) HMIST6, HMISTM6, HMIG3U, HMIG3X, HMISTO7 series with EcoStruxureTM Operator Terminal Expert runtime
  - PFXST6000, PFXSTM6000, PFXSP5000, PFXGP4100 series with Pro-face BLUE runtime

Note: Refer to Schneider Electric advisory for mitigations and more information

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2024-345-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-345-02.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-345-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-345-03.pdf