مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in mySCADA myPRO Manager

Tracking #:432316879

Date:18-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a series of critical vulnerabilities have been discovered in mySCADA's myPRO Manager that could expose industrial operations to severe risks, allowing attackers to perform various malicious actions.

TECHNICAL DETAILS:

A series of critical vulnerabilities have been discovered in mySCADA's myPRO Manager. These vulnerabilities expose industrial operations to severe risks, allowing attackers to execute arbitrary operating system commands, upload malicious files, exfiltrate sensitive information, and gain unauthorized access to critical systems – all without valid credentials. Four vulnerabilities have been disclosed, with two rated as **Critical** (CVSS scores of 9.8 and 10.0), one as **High** (CVSS score of 8.6), and one as **Medium** (CVSS score of 6.3).

Details of the Vulnerabilities:

1. **CVE-2025-25067 (CVSS 9.8 – Critical): OS Command Injection**
   - **Description:** A remote attacker can execute arbitrary operating system commands on the affected system.
   - **Impact:** This could lead to full system compromise, allowing attackers to manipulate industrial processes, steal data, or deploy malware.
2. **CVE-2025-24865 (CVSS 10.0 – Critical): Missing Authentication in Administrative Web Interface**
   - **Description:** The administrative web interface lacks authentication, enabling unauthorized access.
   - **Impact:** Attackers can retrieve sensitive information, upload malicious files, and modify system configurations without requiring credentials.
3. **CVE-2025-22896 (CVSS 8.6 – High): Cleartext Storage of Sensitive Credentials**
   - **Description:** Credentials are stored in cleartext within the system.
   - **Impact:** If attackers gain access to the system, they can easily extract and misuse these credentials to escalate privileges or move laterally within the network.
4. **CVE-2025-23411 (CVSS 6.3 – Medium): Cross-Site Request Forgery (CSRF)**
   - **Description:** The system is vulnerable to CSRF attacks, where an attacker can trick a user into performing unintended actions.
   - **Impact:** This could lead to unauthorized changes to system settings or the theft of sensitive information.

- **Affected versions:**
  - myPRO Manager: Versions prior to 1.4

- **Fixed Versions:**
  - myPRO Manager v1.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade mySCADA myPRO Manager to the fixed version or latest version.

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.myscada.org/downloads/mySCADAPROManager/