مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Schneider Electric Products

Tracking #:432316752

Date:16-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has obsreved multiple vulnerabilities in Schneider Electric products that could potentially be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Schneider Electric has identified multiple vulnerabilities across various products and solutions. Successful exploitation of these vulnerabilities could result in serious consequences, including denial of service, unauthorized access, remote code execution, or exposure of sensitive information.

Vulnerabilities and Affected Products:

1. **Modicon M580 PLCs, BMENOR2200H, and EVLink Pro AC**
   - **CVE**: CVE-2024-11425
   - **Description**: CWE-131: Incorrect Calculation of Buffer Size
   - **Affected Products**:
     - Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety)
     - Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)
     - BMENOR2200H
     - EVLink Pro AC
2. **Pro-face GP-Pro EX and Remote HMI**
   - **CVE**: CVE-2024-12399
   - **Description**: CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel
   - **Affected Products**:
     - Pro-face GP-Pro EX (All versions)
     - Pro-face Remote HMI (All versions)
3. **Wind River VxWorks DHCP Server Vulnerability**
   - **Description**: Vulnerability within the VxWorks Operating System from Wind River.
   - **Affected Products**:
     - Modicon M580 communication modules (BMENOC, BMECRA)
     - Modicon Quantum communication modules (BMXCRA, 140CRA)
4. **Web Designer for Modicon Communication Modules**
   - **CVE**: CVE-2024-12476
   - **Description**: CWE-611: Improper Restriction of XML External Entity Reference
   - **Affected Products**:
     - Web Designer for BMXNOR0200H, BMXNOE0110(H), BMENOC0311(C), BMENOC0321(C)
5. **Web Server on Modicon M340 and Communication Modules**
   - **CVE**: CVE-2024-12142
   - **Description**: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
   - **Affected Products**:
     - Modicon M340 processors (BMXP34*)
     - BMXNOE0100, BMXNOE0110, BMXNOR0200H
6. **RemoteConnect and SCADAPack x70 Utilities**
   - **CVE**: CVE-2024-12703
   - **Description**: CWE-502: Deserialization of Untrusted Data

- **Affected Products**: RemoteConnect and SCADAPackTM x70 Utilities (All versions)

7. **FlexNet Publisher Vulnerability**
   - **Description**: Vulnerability disclosed in Revenera FlexNet Publisher component.
   - **Affected Products**:
     - EcoStruxure™ Control Expert, Process Expert, OPC UA Server Expert, Control Expert Asset Link, Machine SCADA Expert Asset Link, Architecture Builder, Operator Terminal Expert, Machine Expert (including Safety), Machine Expert Twin, Vijeo Designer, and Zelio Soft 2.
8. **PowerLogic™ HDPM6000 High-Density Metering System**
   - **CVE**:
     - CVE-2024-10497: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
     - CVE-2024-10498: CWE-639: Authorization Bypass Through User-Controlled Key
   - **Affected Products**: PowerLogic™ HDPM6000 Version v0.62.7 and prior
9. **EcoStruxure™ Power Build Rapsody**
   - **CVE**: CVE-2024-11139
   - **Description**: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
   - **Affected Products**: EcoStruxure™ Power Build Rapsody
10. **BadAlloc Vulnerabilities**
    - **CVE**: CVE-2020-28895, CVE-2020-35198, CVE-2021-22156
    - **Description**: Multiple memory allocation vulnerabilities may result in denial of service or remote code execution.

Note: Refer to Schneider Electric's official Security Notifications for detailed information on mitigation steps, affected product versions, and available patches.

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://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp