Schneider Electric Security Notification

Easergy T200 Multiple Vulnerabilities

12 March 2024

Overview

Schneider Electric is aware of multiple vulnerabilities in its Easergy T200 products.

The Easergy T200 RTU Product Line (T200I, T200E, T200P) is a modular platform for medium voltage and low voltage public distribution network management. Note, this product has been obsoleted since December 31st, 2021, and is no longer available for purchase.

Failure to apply the remediations provided below may allow a brute force attack, which could result in unauthorized data access, and/or compromise of the device.

Affected Products and Models

Product	Version
Easergy T200 (Modbus) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04MOD-07000104** and prior
Easergy T200 (IEC104) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04IEC-07000104** and prior
Easergy T200 (DNP3) *Models: T200I, T200E, T200P, T200S, T200H*	Version **SC2-04DNP-07000104** and prior

Vulnerability Details

CVE ID: **CVE-2024-2051**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause account takeover and unauthorized access to the system when an attacker conducts brute-force attacks against the login form.

Schneider Electric Security Notification

CVE ID: **CVE-2024-2050**

CVSS v3.1 Base Score 8.2 | High| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists when an attacker injects then executes arbitrary malicious JavaScript code within the context of the product.

CVE ID: **CVE-2024-2052**

CVSS v3.1 Base Score 7.5 | High | [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N**]**

CWE-552: Files or Directories Accessible to External Parties vulnerability exists that could allow unauthenticated files and logs exfiltration and download of files when an attacker modifies the URL to download to a different location.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

Affected Product & Version	Remediation
Easergy T200 Any Model *(Modbus)* *Version **SC2-04MOD-07000104** and prior*	Easergy T200 has reached its end of life. There is a fix for this vulnerability and is available by contacting the Customer Care Center. Customers could also consider upgrading to the latest product offering PowerLogic™ T300 to resolve this issue.
Easergy T200 Any Model *(IEC104)* *Version **SC2-04IEC-07000104** and prior*	
Easergy T200 Any Model *(DNP3)* *Version **SC2-04DNP-07000104** and prior*	

After upgrade, the device will reboot automatically.

The firmware version is displayed in the "Communication Software Information" web page for verification.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2024-2050 CVE-2024-2051 CVE-2024-2052	Tony Marcel Nasr

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, visit the company’s cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0.0 *12 March 2024*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2024.04.01 09:56:48 -04'00'