Schneider Electric Security Notification

Easergy T200

13 July 2021

Overview

Schneider Electric is aware of a vulnerability in its Easergy T200 RTU (Remote Terminal Unit).

The Easergy T200 RTU is a modular platform for medium voltage and low voltage public distribution network management.

Failure to apply the mitigations provided below may allow authentication bypass during control command.

Affected Products and Versions

The communication board is impacted by this vulnerability and is the same for all T200 models (T200I/T200E, T200P). The corresponding firmware depends on the protocol used.

Impacted firmware versions are described in the table below:

Product	Version
Easergy T200 (Modbus)	SC2-04MOD-07000100 and earlier
Easergy T200 (IEC104)	SC2-04IEC-07000100 and earlier
Easergy T200 (DNP3)	SC2-04DNP-07000102 and earlier

Vulnerability Details

CVE ID: **CVE-2021-22772**

CVSS v3.1 Base Score 9.1 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause unauthorized operation when authentication is bypassed.

Remediation

Affected Product & Version	Remediation
Easergy T200 (Modbus)	Customers are strongly encouraged to upgrade to version **SC2-04MOD-07000103** available from the Schneider Electric Customer Care Center.
Easergy T200 (IEC104)	Customers are strongly encouraged to upgrade to version **SC2-04IEC-07000103** available from the Schneider Electric Customer Care Center.
Easergy T200 (DNP3)	Customers are strongly encouraged to upgrade to version **SC2-04DNP-07000103** available from the Schneider Electric Customer Care Center.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure.

Contact Schneider Electric's Customer Care Center if you need assistance.

We also recommend using strong passwords and apply the following rules:

- Change the default passwords the first time you connect to the product
- Renew passwords with reasonable frequency
- Do not store passwords in a file on a computer station that is particularly exposed to risk
- Passwords should be at least 8 characters long and of different types (upper case, lower case, numbers, special characters)

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 for the devices that it is intended for.
- 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.

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

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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *13 July 2021*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2021.07.11 20:17:39 -04'00'