

# Schneider Electric Security Notification

## Easergy T300

11 January 2022

### Overview

Schneider Electric is aware of a vulnerability in the Easergy T300 RTU (Remote Terminal Unit).

The [Easergy T300](#) is a modular platform for medium voltage and low voltage public distribution network management.

Failure to apply the mitigations provided below may allow for arbitrary code execution, which could result in denial of service.

### Affected Products and Versions

Product	Version
<b>Easergy T300</b>  Note: Only products connected to a 3G/4G network using the following T300 modems are vulnerable: <ul style="list-style-type: none"><li>- <b>Easergy HU250 3G modem box - Five Bands UMTS/HSPA+</b> (see modem on se.com <a href="#">here</a>)</li><li>- <b>Easergy HU250 4G modem box with GPS clock synchronization</b> (see modem on se.com <a href="#">here</a>)</li></ul>	Firmware V2.7.1 and prior

### Vulnerability Details

CVE ID: **CVE-2020-8597**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H

A point-to-point (pppd) communication library deployed with the T300 is vulnerable to [CVE-2020-8597](#), a *CWE-120: Buffer Copy without Checking Size of Input* vulnerability, which may allow for arbitrary code execution and lead to a denial of service when an attacker gains access to a connected cellular network. The CVSS score, provided above, is evaluated as Medium in the product context.

### Remediation

Easergy T300 firmware V2.8 includes a fix for this vulnerability and is available from the Schneider Electric [Customer Care Center](#).

Note: The 3G/4G hardware is optional and the feature is disabled by default. In case this feature is used as a communication channel, it is recommended to disable it until the firmware is upgraded.

# Schneider Electric Security Notification

## 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.

## 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,

## Schneider Electric Security Notification

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](http://www.se.com)

Revision Control:

<b>Version 1.0</b> <i>11 January 2022</i>	<b>Original Release</b>
--	-------------------------