# Schneider Electric Security Notification

## Easergy T300 (V2.0)

**10 November 2020 (8 December 2020)**

## Overview

Schneider Electric is aware of a vulnerability in its 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 remediation provided below may allow unauthorized access to the internal product LAN (local area network).

December 2020 Update: Additional CVEs have been added to this disclosure (marked in red). No additional action is required for customers who have already followed the remediation instructions provided below.

## Affected Products and Versions

Easergy T300 with firmware 2.7 and older

## Vulnerability Details

CVE ID: **CVE-2020-7561**

CVSS v3.0 Base Score 10 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause a wide range of problems, including information exposure, denial of service, and command execution when access to a resource from an attacker is not restricted or incorrectly restricted.

CVE ID: **CVE-2020-28215**

CVSS v3.0 Base Score 7.7 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H

A CWE-862: Missing Authorization vulnerability exists that could cause a wide range of problems, including information exposures, denial of service, and arbitrary code execution when access control checks are not applied consistently.

CVE ID: **CVE-2020-28216**

CVSS v3.0 Base Score 7.6 | High | CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that would allow an attacker to read network traffic over HTTP protocol.

CVE ID: **CVE-2020-28217**

CVSS v3.0 Base Score 6.7 | Medium | CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L

A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that would allow an attacker to read network traffic over IEC60870-5-104 protocol.

CVE ID: **CVE-2020-28218**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:L

A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists that would allow an attacker to trick a user into initiating an unintended action.

## Remediation

Customers are strongly encouraged to upgrade to V2.7.1 available from the Schneider Electric Customer Care Center. Alternatively, they may disable port forwarding in the product firewall.

## 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.

# Schneider Electric Security Notification

## Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

| CVE | Researchers |
|---|---|
| CVE-2020-7561, CVE-2020-28215 | Evgeniy Druzhinin and Ilya Karpov of Rostelecom-Solar |

## 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. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

# Schneider Electric Security Notification

## 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**<br>*10 November 2020* | Original Release |
| **Version 2.0**<br>*8 December 2020* | Added the following CVEs: *CVE-2020-28215, CVE-2020-28216, CVE-2020-28217, CVE-2020-28218.* Updated CWE for CVE-2020-7561. (page 1-2). |

Product Security Office

Digitally signed by Product Security Office
Date: 2020.12.06 13:53:52 -05'00'