Life Is On Schneider Electric

Schneider Electric Security Notification

Easergy T300 (V1.1)

9 June 2020 (13 May 2021)

Overview

Researchers from Rostelecom-Solar have made Schneider Electric aware of multiple vulnerabilities affecting the company's Easergy T300 product. Schneider Electric has worked closely with the researchers to remediate the vulnerabilities. We appreciate their collaboration and commitment to transparency. The vulnerabilities have been remediated via a free firmware update, which is available immediately by contacting Schneider Electric's Customer Care Center.

Access to the customer's network is required for the majority of the disclosed vulnerabilities to be exploited. Therefore, if the customer's network is well protected and monitored for intrusion, and care is taken to obtain software updates from a trusted source, the general risk of exploitation can be substantially minimized.

Schneider Electric encourages customers to upgrade to the new firmware as soon as possible. The company further encourages customers to ensure any firmware files used to update the device are acquired from trusted sources; to operate the products on properly segmented control networks; to adequately secure any workstation that has been configured to have access to the product; and to follow the remediation and general security recommendations below.

Affected Products

Easergy T300 with firmware 1.5.2 and older

T300 is a grid automation platform that is typically deployed to medium voltage (2400-69000 VAC) substation cabinets.

Vulnerability Details

CVE ID: **CVE-2020-7503**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists which could allow an attacker to execute malicious commands on behalf of a legitimate user when xsrf-token data is intercepted.

Schneider Electric Security Notification

CVE ID: **CVE-2020-7504**

CVSS v3.0 Base Score 5.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

A CWE-20: Improper Input Validation vulnerability exists which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent.

CVE ID: **CVE-2020-7505**

CVSS v3.0 Base Score 6.1 | Medium | CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:H

A CWE-494 Download of Code Without Integrity Check vulnerability exists which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system.

CVE ID: **CVE-2020-7506**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-200: Information Exposure vulnerability exists which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure.

CVE ID: **CVE-2020-7507**

CVSS v3.0 Base Score 9.3 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H

A CWE-400: Uncontrolled Resource Consumption vulnerability exists which could allow an attacker to login multiple times resulting in a denial of service.

CVE ID: **CVE-2020-7508**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists which could allow an attacker to gain full access by brute force.

CVE ID: **CVE-2020-7509**

CVSS v3.0 Base Score 9.0 | Critical | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H

A CWE-269: Improper privilege management (write) vulnerability exists which could allow an attacker to elevate their privileges and delete files.

CVE ID: **CVE-2020-7510**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

A CWE-200: Information Exposure vulnerability exists which could allow attacker to obtain private keys.

CVE ID: **CVE-2020-7511**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists which could allow an attacker to acquire a password by brute force.

CVE ID: **CVE-2020-7512**

CVSS v3.0 Base Score 5.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-1103: Use of Platform-Dependent Third Party Components with vulnerabilities vulnerability exists which could allow an attacker to exploit the component.

CVE ID: **CVE-2020-7513**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists which could allow an attacker to intercept traffic and read configuration data.

Remediation

This vulnerability is fixed in T300 firmware version 2.7 and is available from your Schneider Electric Customer Care Center.

Additionally, Schneider Electric recommends customers apply the following mitigations to further reduce risk:

- Ensure firmware is obtained from a trusted source and integrity is protected.
- Use a separate secure local network and use secure computer access controls.

Schneider Electric Security Notification

Product Information

The Easergy T300 RTU is a modular platform of hardware and firmware and an application building block for Medium Voltage and Low Voltage public distribution network management. It is typically deployed to medium voltage (2400-69000 VAC) substation cabinets.

Product Category - Medium Voltage Distribution and Grid Automation

Learn more about Schneider Electric's product categories here: http://www.se.com/us/en/all-products

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 laptops 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.

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-2020-7503, CVE-2020-7504, CVE-2020-7505, CVE-2020-7506, CVE-2020-7507, CVE-2020-7508, CVE-2020-7509, CVE-2020-7510, CVE-2020, 7511, CVE-2020-7512, CVE-2020-7513	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, please contact your local Schneider Electric representative and/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

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, ensuring **Life Is On** everywhere, for everyone, at every moment.

Schneider Electric Security Notification

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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *9-Jun-2020*	Original Release
Version 1.1 *13-May-2021*	Updated CWE for CVE-2020-7506

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.13 18:22:08 -04'00'