Schneider Electric Security Notification

Schneider Electric Software Update (SESU) – SUT Service component

13 August 2019

Overview

Schneider Electric is aware of a vulnerability in the Schneider Electric Software Update (SESU) – SUT Service component.

A possible exploitation could allow an attacker to execute arbitrary code on the targeted system with SYSTEM privileges.

Affected Product(s)

Schneider Electric Software Update (SESU) SUT Service component - from versions 2.1.1 to v2.3.0.

Vulnerability Details

CVE ID: **CVE-2019-6834**

CVSS v3.0 Base Score 7.3 | (High) | CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

A CWE-502: Deserialization of Untrusted Data vulnerability exists which could allow an attacker to execute arbitrary code on the targeted system with SYSTEM privileges when placing a malicious file at a certain location on the filesystem. By default, this folder location requires the malicious user to be authenticated for this vulnerability to be successfully exploited.

Remediation

This vulnerability is fixed in version 2.3.1 and is available for download below:

https://www.seupdate.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_231/SESU_2.3.1_setup_sfx.exe

To install the security update please download and execute the setup file.

The following mitigation can be applied by customers to reduce the risk:

- Restrict write access to the folder “%ProgramData%\Schneider Electric”.

Product Information

Schneider Electric Software Update (SESU) offers two main features for Schneider Electric software products:

1. It automatically notifies customers on the availability of hotfixes or new versions and makes it easy to download and install such updates.

2. It implements the Schneider Electric software improvement program by uploading some anonymous data from the customer PC (see Schneider Electric Data Privacy Statement).

Schneider Electric Software Update (SESU) is used by the following products:

- AltistartDTMLibrary
- AltivarATV320DTMLibrary
- AltivarDTMLibrary
- AltivarMachine340DTMLibrary
- AltivarProcessATV6xxDTMLibrary
- AltivarProcessATV9xxDTMLibrary
- Compact NSX Firmware Update
- eConfigure
- EcoStruxure Augmented Operator Advisor
- EcoStruxure Control Expert
- EcoStruxure Hybrid DCS
- EcoStruxure Machine Expert
- EcoStruxure Machine Expert Basic
- EcoStruxure Machine Expert HVAC
- EcoStruxure Operator Terminal Expert
- EcoStruxure Plant Builder
- EcoStruxure Power Commission
- Eurotherm Data Reviewer
- eXLhoist Configuration Software
- HarmonyXB5SSoft
- Lexium 26 DTM Library
- Lexium 28 DTM Library
- Lexium 32 DTM Library
- Schneider Electric Easergy Studio
- Schneider Electric Floating License Manager
- Schneider Electric License Manager
- Schneider Electric Motion Sizer
- Schneider Electric SQL Gateway

- Schneider Electric TeSys Island DTM Library
- SoMachine Basic
- SoMachine Motion Software
- SoMachine Motion Tools
- SoMachine Software
- SoMove
- SoSafe Configurable
- SoSafe Programmable
- TeSys DTM Library
- Unity M580 Application Converter (UMAC)
- Unity Loader
- Unity Pro
- Vijeo Designer
- Vijeo XD
- Zelio Soft

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

In the Windows Control Panel App, open the section "Programs > Programs and Features". You are affected if you have installed any version of Schneider Electric Software Update (SESU) from version 2.1.1 up to 2.3.0.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.

- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6834	Amir Preminger (Claroty)

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.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. 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 *13 Aug 2019*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2019.08.12 14:08:00 -04'00'