Life Is On Schneider Electric

Schneider Electric Security Notification

Schneider Electric Software Update (SESU)

14 July 2020

Overview

Schneider Electric is aware of a vulnerability in the Schneider Electric Software Update (SESU) product.

Affected Product(s)

Schneider Electric Software Update (SESU) V2.4.0 and prior.

Schneider Electric Software Update is used by the following products*:

- EcoStruxure Augmented Operator Advisor
- EcoStruxure Control Expert (formerly known as Unity Pro)
- EcoStruxure Hybrid Distributed Control System (DCS)
- EcoStruxure Machine Expert (formerly known as SoMachine)
- EcoStruxure Machine Expert Basic
- EcoStruxure Operator Terminal Expert
- Eurotherm Data Reviewer
- Eurotherm iTools
- eXLhoist Configuration Software
- Schneider Electric Floating License Manager
- Schneider Electric License Manager
- Harmony XB5SSoft
- SoMachine Motion
- SoMove
- Versatile Software BLUE
- Vijeo Designer
- OsiSense XX Configuration Software
- Zelio Soft 2

*Note: includes but not limited to the offers listed

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-7520**

CVSS v3.0 Base Score 7.9 | High | CVSS V3.0: AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:H/A:H

A CWE-601: URL Redirection to Untrusted Site ('Open Redirect') vulnerability exists which could cause execution of malicious code on the victim´s machine. In order to exploit this vulnerability, an attacker requires privileged access on the engineering workstation to modify a Windows registry key which would divert all traffic updates to go through a server in the attacker's possession. A man-in-the-middle attack is then used to complete the exploit.

Remediation

This vulnerability is fixed in version 2.5.0 and is available for download below:

https://www.seupdate.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_250/SESU_2.5.0_setup_sfx.exe

If you have already installed SESU, it will show that a new critical update is available for installation. To install the security update, download and execute the setup file.

Product Information

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

1. It notifies customers about 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).

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here:
https://www.se.com/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 potentially affected if you have installed any version of Schneider Electric Software Update (SESU) up to V2.4.0.

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 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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2020-7520	Amir Preminger (VP Research) of Claroty

Schneider Electric Security Notification

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 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

Legal Disclaimer

Revision Control:

Version 1 *14 July 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.07.11 00:18:54 -04'00'