Schneider Electric Security Notification

Schneider Electric Software Update

9 November 2021

Overview

Schneider Electric is aware of a vulnerability in its Schneider Electric Software Update product (also referred to as “SESU”), which is used to notify and download updates for other Schneider Electric Software products.

To connect to the Internet, the SESU product offers users to manually configure the proxy settings. Due to an improper protection of the saved credentials, it is potentially possible for an attacker to decrypt these credentials.

Affected Product and Versions

Schneider Electric Software Update, V2.3.0 through V2.5.1

Vulnerability Details

CVE ID: **CVE-2021-22799**

CVSS v3.1 Base Score 3.8 | Low | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

A CWE-331: Insufficient Entropy vulnerability exists that could cause unintended connection from an internal network to an external network when an attacker manages to decrypt the SESU proxy password from the registry.

Remediation

The version V2.5.2 of the SESU product includes a fix for this vulnerability and is available for download here:

https://www.seupdate.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_latest_version/SESU_latest_setup_sfx.exe

Note: This link will always be updated to point to the latest version of SESU

If you have already installed SESU and activated notification of updates, it will show that a new security patch is available for installation. To install the security update, which is strongly recommended, download and execute the setup file. However, as long as versions 2.3.0 - 2.5.1 of SESU are installed and configured to use a manually defined proxy server with credentials, make sure only authorized users, which are allowed to see them, have access to this machine. If this cannot be guaranteed, make sure no proxy credentials are stored.

Schneider Electric Security Notification

Affected Products	Remediation
Schneider Electric Software Update is used by the following products*: • EcoStruxure Augmented Operator Advisor • EcoStruxure Control Expert (formerly known as Unity Pro) • EcoStruxure Process Expert (formerly known as EcoStruxure Hybrid Distributed Control System) • EcoStruxure Machine Expert (formerly known as SoMachine or SoMachine Motion) • EcoStruxure Machine Expert Basic • EcoStruxure Operator Terminal Expert • EcoStruxure Plant Builder • EcoStruxure Power Design • EcoStruxure Automation Expert • EcoStruxure Automation Maintenance Expert • Eurotherm Data Reviewer • Eurotherm iTools • eXLhoist Configuration Software • Schneider Electric Floating License Manager • Schneider Electric License Manager • Harmony XB5SSoft • SoMove • Versatile Software BLUE • Vijeo Designer • OsiSense XX Configuration Software • Zelio Soft 2 *Note: includes but not limited to the offers listed; some of the products might not deliver SESU as part of the product package, however SESU can be downloaded and used to manage the product updates. It may also be possible that more components for one product are listed in the “SESU Managed Products” dialog for update.	If SESU is installed (assuming SESU is configured as “managed product” inside the SESU application) it will indicate that a security update is available. Click to download and install the new SESU version. If SESU is not installed, follow the link download SESU and follow the installation instructions. https://www.seupdate.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_latest_version/SESU_latest_setup_sfx.exe

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric’s Customer Care Center if you need assistance removing a patch.

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.

Acknowledgements

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

CVE	Researcher
CVE-2021-22799	Nozomi Networks via ICS-CERT/CISA

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.

Schneider Electric Security Notification

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, 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

Revision Control

Version 1.0 *9 November 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.11.06 01:22:26 -04'00'