

Schneider Electric Security Notification

SoMove

11 August 2020

Overview

Schneider Electric is aware of a vulnerability in the SoMove application.

Affected Product(s)

SoMove V2.8.1 and prior

Vulnerability Details

CVE ID: **CVE-2020-7527**

CVSS v3.0 Base Score 4.0 | Medium | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

A CWE-276: Incorrect Default Permission vulnerability exists which could cause elevation of privilege and provide full access control to local system users to SoMove component and services when a SoMove installer script is launched.

Remediation

This vulnerability is fixed in SoMove V2.8.2 and is available for download below:

https://www.se.com/ww/en/download/document/SoMove_FDT/

The following mitigations and workarounds can be applied by customers to reduce the risk:

- Manually update the access control permissions in the folder C:\Program Files (x86)\Schneider Electric\SoMove by providing read only permission to users. This setting will prevent everyone from overwriting file content without privileges.

Product Information

SoMove is a setup software for motor control devices, designed to configure motor control devices (Altivar, Altistart, Lexium and Tesys product lines).

Schneider Electric Security Notification

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

SoMove V2.8.1 and prior

Note: The version information can be found on SoMove application banner.

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 to prevent unauthorized personnel from accessing 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 target network.
- 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 been connected to any network other than the intended network to connect to the intended networks without proper sanitation.
- Minimize network exposure to all control 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-2020-7527	Luis Alvernaz

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 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>

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 **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 <i>11 August 2020</i>	Original Release
---	-------------------------