Life Is On Schneider Electric

Schneider Electric Security Notification

Security Notification – Schneider Electric Modbus Serial Driver

9 April 2019

Overview

Schneider Electric has become aware of a vulnerability in the Modbus Serial Driver component.

Affected Product(s)

Modbus Serial Driver version:

- For 64-bit Windows OS: **V3.17 IE 37** and prior
- For 32-bit Windows OS: **V2.17 IE 27** and prior
- As part of the Driver Suite version: V14.12 and prior

NOTE: Modbus Serial Driver component depends on Drivers Manager component, both are parts of the Driver Suite. Modbus Serial Driver version is visible in the "Modbus Serial Driver"-Tab of the Drivers Manager. Start the Drivers Manager in Windows Control Panel -> Drivers Manager.

Vulnerability Details

CVE ID: **CVE-2018-7824**

CVSS Score: 7.8 | (High) | CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

An Externally Controlled Reference to a Resource (CWE-610) vulnerability exists which could allow write access to system files available only to users with SYSTEM privilege or other important user files.

Remediation

A fix for this vulnerability is available for download below:

https://www.schneider-electric.com/en/download/document/SEModbusDriverSuite/

Schneider Electric Security Notification

Setup file of Modbus SL Driver - SchneiderModbusDriverSuite V14.13.0.0

- Win 7 / 8 / 8.1 / 10, 32-bit
- Win 7 / 8 / 8.1 / 10, 64-bit
- Win Server 2012 R2 / 2016, 64-bit

Please download and execute the setup file.

Schneider Modbus Driver Release Notes

https://www.schneider-electric.com/en/download/document/MD_RN/

Product Information

The Modbus Serial Driver is used by the following products:

- TwidoSuite
- PowerSuite
- SoMove
- SoMachine
- Unity Pro
- Control Expert
- Unity Loader
- Concept
- Modbus SL Comm DTM
- PL7
- SFT2841
- OFS

Industry Sector

Industrial Automation Control

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 would like to recognize the following researcher(s) for all their efforts related to identification and coordination of this vulnerability:

CVE	Researcher(s) Name
CVE-2018-7824	Reid Wightman (Dragos)

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, please visit the company’s cybersecurity web page:

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

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 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

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *9 April 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.04.09 12:46:34 -04'00'