Schneider Electric Security Notification

Schneider Electric Modbus Serial Driver

11 August 2020 (13 October 2020)

Overview

Schneider Electric is aware of a vulnerability in the Modbus Serial Driver Component.

Affected Products and Versions

- Schneider Electric Modbus Serial Driver (64 bits) versions prior to **V3.20 IE 30**.
- Schneider Electric Modbus Serial Driver (32 bits) versions prior to **V2.20 IE 30**.
- Schneider Electric Modbus Driver Suite versions prior to **V14.15.0.0.**

The Modbus Serial Driver is used by the following products*:

- Ecostruxure Control Expert (formerly known as Unity Pro)
- Unity Loader
- EcoStruxure Process Expert (formerly known as Hybrid DCS)
- EcoStruxure OPC UA Server Expert
- OPC Factory Server
- Advantys Configuration Software
- Modbus Communications DTM (Field Devices)
- SoMove
- Ecostruxure Machine Expert (formerly known as SoMachine)
- Ecostruxure Machine Expert Basic
- Harmony® eXLhoist
- EcoStruxure Power Commission

Customers using these products should apply the steps in the Remedation section below.

* Includes but is not limited to the offers listed

Vulnerability Details

CVE ID: **CVE-2020-7523**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

A CWE-269: Improper Privilege Management vulnerability exists which could cause local privilege escalation when the Modbus Serial Driver service is invoked. The driver does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.

Remediation

Modbus Serial Driver

This vulnerability is fixed in Schneider Electric Modbus Driver Suite version V14.15.0.0 and is available for download below:

https://www.se.com/ww/en/download/document/MSCD_V14.15.0.0/

The Schneider Electric Modbus Driver Suite is an independent software component which will fix this vulnerability in all affected products.

Please download install package and release notes and execute the Setup file.

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

- Follow workstation, network, and site-hardening guidelines in the Cybersecurity Best Practices guide available for download here.

Note: For EcoStruxure Power Commission, the updated Modbus Serial Driver is included in V6.0 and is available for download below:

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

Note: For EcoStruxure Machine Expert Basic, the updated Modbus Serial Driver is included in V1.1 and is available for download below:

https://www.seupdate.schneider-electric.com/download/MachineExpertBasic/MachineExpertBasic-V1.1.0/MachineExpertBasic_V1.1_build64712.exe

Product Information

Schneider Electric Modbus Serial Driver is used by Schneider Electric products to communicate with devices using the Modbus Serial protocol.

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:

Schneider Electric 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.

The Modbus Serial Driver component depends on Drivers Manager component. Both are parts of the Schneider Electric Modbus Driver Suite, which represents the installation package.

It is either installed by default or optionally as part of the product installation procedure (see the list of products above), but it can also be installed separately.

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-2020-7523	Nicolas DELHAYE (Airbus Cybersecurity)

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

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 *11 August 2020*	Original Release
Version 1.1 *13 October 2020*	-Added Remediation note for *EcoStruxure Machine Expert Basic* -Minor formatting changes

Product Security Office

Digitally signed by Product Security Office
Date: 2020.10.09 16:56:14 -04'00'