Important security notification – Schneider Electric Modbus Driver Vulnerability

April 3, 2014

Schneider Electric® has become aware of a vulnerability involving its Modbus Serial driver.

The vulnerability identified:

Several Schneider Electric® software products (see list below) bundle the Schneider Electric® Modbus Serial Driver (ModbusDrv.exe), which is started when attempting to connect to a Programmable Logic Controller (PLC) via the serial port of a PC; e.g. when in "Monitoring" mode or when opening an existing project on a PLC in "Programming" mode.

Under certain conditions which would require a multi-step process, an internal buffer overflow condition could be created. An attacker could gain control of the program flow and execute arbitrary code with the permissions of the user running any of the software products listed below. There is no evidence that this vulnerability has been exploited in the field.

Schneider Electric takes these vulnerabilities seriously and has devoted resources to investigate and address these issues. We believe it is critical to consider the whole picture including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following products are affected by the vulnerability of the Modbus Serial Driver

Windows Platform and Modbus Serial Driver version

Windows OS version	Modbus Serial Driver
XP 32 bit	V1.10 IE v37
Vista 32 bit	2.2 IE12
Windows 7 32 bit	2.2 IE12
Windows 7 64 bit	3.2 IE12

Schneider Electric Product and version

Product	Version
TwidoSuite	2.31.04 and prior
PowerSuite	2.6 and prior
SoMove	V1.7 and prior
SoMachine	V2.0, V3.0, V3.1, V3.0 XS
Unity Pro	V7.0 and prior

UnityLoader	V2.3 and prior
Concept	V2.6 SR7 and prior
ModbusCommDTM sl	V 2.1.2 and prior
PL7	V4.5 SP5 and prior
SFT2841	V 14; V13.1 and prior
OFS	~~V3.50~~ V3.40 and prior

Details on Mitigations and Workarounds

OFS V3.5 and Unity Pro V8 have been released including the updated ModbusDriverSuite. For other products listed, the updated ModbusDriverSuite will be implemented with each new version of those Software Products. Until the ModbusDriverSuite becomes available, Schneider Electric recommends using a firewall to allow only authorized systems to access these applications.

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://download.schneider-electric.com/files?p_Doc_Ref=STN v2

Acknowledgments

Schneider Electric wishes to thank the researcher, Carsten Eiram, for reporting the vulnerability and working with Schneider Electric during the disclosure process.

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

CVSS Base Score: 9.3   AV:N/AC:M/Au:N/C:C/I:C/A:C

For More Information

This document is intended to help provide an overview of the identified vulnerability 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 on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at

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

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com