

Schneider Electric Security Notification

Modicon Controllers

8 October 2019

Overview

Schneider Electric is aware of a vulnerability in four of its Modicon brand of programmable logic controllers.

Affected Product(s)

- Modicon M580 (all firmware versions)
- Modicon M340 (all firmware versions)
- Modicon Premium (all firmware versions)
- Modicon Quantum (all firmware versions)

Vulnerability Details

CVE ID: **CVE-2019-6845**

CVSS v3.0 Base Score 5.9 | (Medium) | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists, which could cause the disclosure of information when transferring applications to the controller using Modbus TCP protocol.

Remediation

The vulnerabilities described in this document are linked to weaknesses in the management of the Modbus communications protocol. Customers are strongly recommended to implement the mitigations listed below to reduce risk.

Modicon M580:

To mitigate the risks associated with weaknesses in the Modbus protocol, users should immediately:

- Set up network segmentation and implement a firewall to block all unauthorized access to port 502/TCP.
- Set up a secure communication according to the “Modicon Controllers Platform Cyber Security Reference Manual” guidelines (see the chapter “Setup Secured Communications” available here:

Schneider Electric Security Notification

<https://www.schneider-electric.com/en/download/document/EIO0000001999/>

- Use a BMENOC module and follow the instructions to configure the IPSEC feature as described in the guideline “Modicon M580 - BMENOC03.1 Ethernet Communications Module, Installation and Configuration Guide” in the chapter “Configuring IPSEC communications”:

<https://www.schneider-electric.com/en/download/document/HRB62665/>

Modicon M340:

To mitigate the risks associated with weaknesses in the Modbus protocol, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP.

Modicon Premium:

To mitigate the risks associated with weaknesses in the Modbus protocol, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP.

Modicon Quantum:

Schneider Electric’s Modicon Quantum controllers have reached their end of life and are no longer commercially available. They have been replaced by the [Modicon M580 ePAC](#) controller, our most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

To mitigate the risks associated with weaknesses in the Modbus protocol, users should immediately:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP

Product Information

Ethernet Programmable Automation Controller for industrial process and infrastructure

Product Category - All Categories

Learn more about Schneider Electric’s product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

Affected products listed in this security notification connected to an Ethernet network

Schneider Electric Security Notification

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 recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6845	Jared Rittle (Cisco Talos)

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.

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

Schneider Electric Security Notification

<https://www.schneider-electric.com/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:

<p>Version 1 8-Oct-19</p>	<p>Original Release</p>
--------------------------------------	-------------------------