

Schneider Electric Security Notification

Modicon Controllers

8 October 2019

Overview

Schneider Electric is aware of multiple vulnerabilities in three of its Modicon brand of programmable logic controllers.

Affected Product(s)

- Modicon M580
- Modicon BMENOC 0311
- Modicon BMENOC 0321

Vulnerability Details

CVE ID: **CVE-2019-6848**

CVSS v3.0 Base Score 8.6 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the PLC when sending specific data on the REST API of the controller/communication module.

CVE ID: **CVE-2019-6849**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-200: Information Exposure vulnerability exists, which could cause the disclosure of sensitive information when using specific Modbus services provided by the REST API of the controller/communication module.

CVE ID: **CVE-2019-6850**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-200: Information Exposure vulnerability exists, which could cause the disclosure of sensitive information when reading specific registers with the REST API of the controller/communication module.

Schneider Electric Security Notification

Remediation

The REST API provides another access to the Modbus services of the Modicon controller. However, the REST API interface is just a redirection to the Modbus TCP server and therefore has the same weaknesses Schneider Electric has disclosed in relation to the Modbus TCP.

To mitigate the risks associated to the REST API weaknesses, users should immediately apply the following instructions.

- Set up network segmentation and implement a firewall to block all unauthorized access to port 80/HTTP on the controllers.
- Deactivate the HTTP service when not needed or restrict to authorized users.
- Set up a secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual”, in chapter “Setup secured communications”:

<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/>

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

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.

Schneider Electric Security Notification

- 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-2019-6848, CVE-2019-6849, CVE-2019-6850	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>

<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

Schneider Electric Security Notification

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 8-Oct-19	Original Release
------------------------------	-------------------------