Schneider Electric Security Notification

Web Server on Modicon M580 Controllers and Communication Modules (V3.0)

8 October 2019 (11 May 2021)

Overview

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

The Modicon M580 are PAC and Safety PLCs with built-in Ethernet for process, high availability & safety solutions.

Failure to apply the mitigations and remediations provided below may risk disclosure of sensitive information and denial of service.

May 2021 Update: A fix is now available for CVE-2019-6849 on the BMENOC0311

Affected Products

- Modicon M580 CPU
  - BMEx58*
- Modicon M580 communication modules
  - BMENOC0311, BMENOC0321

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-755: Improper Handling of Exceptional Conditions* 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

Impacted versions:

- **Modicon M580 with firmware version prior to V3.10** – A fix is available for this vulnerability on firmware V3.20, available on the Download Links section.
- **Modicon BMENOC0311 with firmware version prior to 2.17** – A fix is available for this vulnerability on firmware V2.18, available on the Download Links section.
- **Modicon BMENOC0321 with firmware version prior to 1.06** – A fix is available for this vulnerability on firmware V1.07, available on the Download Links section.

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.

Impacted versions:

- **Modicon M580 with firmware version prior to V3.10** – A fix is available for this vulnerability on firmware V3.20, available on the Download Links section.
- **Modicon BMENOC0311 with firmware version prior to V2.19 -** A fix is available for this vulnerability on firmware V2.19, available on the Download Links section.
- **Modicon BMENOC0321, all versions -** See recommendations in the Mitigations section.

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.

Impacted versions

- **Modicon M580, all versions -** See recommendations in the Mitigations section.
- **Modicon BMENOC0311, all versions -** See recommendations in the Mitigations section.
- **Modicon BMENOC0321, all versions -** See recommendations in the Mitigations section.

Mitigations

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/TCP 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/

Download Links Section

M580 CPU BMEx58*	Firmware version 3.20 is available for all the product references. Follow this link and find the right firmware file based on model used. https://www.se.com/ww/en/product-range/62098-modicon-m580/?parent-subcategory-id=3950&selected-node-id=12692239763#tabs-top
BMENOC0311	Firmware version 2.19 is available here: https://www.se.com/ww/en/product/BMENOC0311/ethernet-module-m580---3-port-factorycast-ethernet-communication/
BMENOC0321	Firmware version 1.07 is available here: https://www.se.com/ww/en/product/BMENOC0321/ethernet-module-m580---3-subnets---ip-forwarding-function/

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 for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher 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

About Schneider Electric

Schneider Electric Security Notification

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 1.0 *8 October 19*	Original Release
Version 2.0 *10 November 2020*	Fixes now available for CVE-2019-6848 and CVE-2019-6849 (page 1-3)
Version 2.1 *15 April 2021*	Updated CWE for CVE-2019-6848
Version 3.0 *11 May 2021*	Fix now available for CVE-2019-6849 on the BMENOC0311 (page 1-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 22:44:52 -04'00'