Schneider Electric Security Notification

Security Notification – Modicon Controllers

14 May 2019

Overview

Schneider Electric is aware of a vulnerability in its line of Modicon process controllers and remote I/O product.

Affected Product(s)

- Modicon M580 with firmware prior to V2.50
- Modicon M340 with firmware prior to V3.01
- BMxCRA312xx with firmware prior to V2.40
- Modicon Premium - all firmware versions
- 140CRA312xxx - all firmware versions

Vulnerability Details

CVE ID: **CVE-2018-7851**

CVSS v3.0 Base Score 5.3 | (Medium) | CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

CWE-119: Buffer errors vulnerability exists when sending a specially crafted Modbus packet, which could cause a denial of service to the device that would force a restart to restore availability.

Remediation

A fix for this vulnerability is available in the firmware versions listed below for M580 (V2.50), M340 (V3.01), and BMX/E CRA (V2.40). Mitigations are explained below for Modicon Premium and 140CRA312xxx.

M580 V2.80 firmware	
BMEP584040 BMEP584040S BMEH584040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV2.80/

BMEP586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV2.80/
BMEH586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV2.80/
BMEP581020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV2.80/
BMEP582020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV2.80/
BMEP582040 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80/
BMEP583020	https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV2.80/
BMEP583040	https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV2.80/
BMEP584020	https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV2.80/
BMEP585040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV2.80/
BMEP582040S	https://www.schneider-electric.com/en/download/document/M580_BMEP582040S_SV2.80/
BMEH582040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80

M340 firmware V3.01	
BMXP3420302 and CL and H	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/
BMXP342020 and H	https://www.schneider-electric.com/en/download/document/BMXP342020_Firmwares/

BMXP342000	https://www.schneider-electric.com/en/download/document/BMXP342000_Firmwares/
BMXP341000 and H	https://www.schneider-electric.com/en/download/document/BMXP341000_Firmwares/
BMXP3420102 and CL	https://www.schneider-electric.com/en/download/document/BMXP3420102_Firmwares/
BMXP3420302	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/

BMX/E CRA firmware V2.40	
BMXCRA31210C	https://www.schneider-electric.com/en/download/document/X80_BMXCRA31210_SV2.40/
BMXCRA31210 and C	https://www.schneider-electric.com/en/download/document/X80_BMECRA31210_SV2.40/
BMXCRA31200	https://www.schneider-electric.com/en/download/document/X80_BMXCRA31200_SV2.40/

Modicon Premium and 140CRA312xxx - To mitigate risks of Denial of Service attacks on the remote IO, users should immediately:

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

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.

Product Information

Ethernet Programmable Automation Controller for industrial process and infrastructure, and Ethernet RIO drop adaptors.

Product Category - All Categories

Learn more about Schneider Electric's product categories here: www.schneider-electric.com/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 has 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 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-2018-7851	Nikita Maximov and Alexey Stennikov (Positive Technologies)

For More Information

This document is intended to help provide an overview of the identified situation 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 related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: 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 MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 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

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *14 May 2019*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2019.05.14 22:05:27 -04'00'