

# Schneider Electric Security Notification

## Security Notification – Modicon Controllers

14 May 2019

### Overview

Schneider Electric is aware of a vulnerability affecting some of its Modicon line of process controllers.

### Affected Product(s)

- Modicon M580 firmware versions prior to V2.30
- Modicon M340 firmware - all firmware versions
- Modicon Premium - all firmware versions
- Modicon Quantum - all firmware versions

### Vulnerability Details

CVE ID: **CVE-2019-6821**

CVSS v3.0 Base Score 5.4 | (Medium) | CVSS:3.0/ AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CWE-330: Use of Insufficiently Random Values vulnerability, which could cause the hijacking of the TCP connection when using Ethernet communication.

### Remediation

The most recent versions of the **Modicon M580** firmware (V2.30 and newer) fix this vulnerability. The latest version (V2.80) is available for free download below.

M580 V2.80 Firmware	
BMEP584040 BMEP584040S BMEH584040 and C	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV2.80/</a>
BMEP586040 and C	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV2.80/</a>
BMEH586040 and C	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV2.80/</a>

## Schneider Electric Security Notification

BMEP581020 and H	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV2.80/</a>
BMEP582020 and H	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV2.80/</a>
BMEP582040 and H	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80/</a>
BMEP583020	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV2.80/</a>
BMEP583040	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV2.80/</a>
BMEP584020	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV2.80/</a>
BMEP585040 and C	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV2.80/</a>
BMEP582040S	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP582040S_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP582040S_SV2.80/</a>
BMEH582040 and C	<a href="https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80/">https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.80</a>

### Modicon M340:

No fix is currently available. To mitigate the risks associated to this TCP protocol weakness, users should immediately:

- Set up network segmentation and implement a firewall to block all remote/external access to TCP ports.
- Configure the Access Control List following the recommendations of the user manual “Modicon M340 for Ethernet Communications Modules and Processors User Manual” chapter “Messaging Configuration Parameters” available at [https://download.schneider-electric.com/files?p\\_enDocType=User+guide&p\\_File\\_Name=31007131\\_K01\\_000\\_16.pdf&p\\_Doc\\_Ref=31007131K01000](https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=31007131_K01_000_16.pdf&p_Doc_Ref=31007131K01000)

### Modicon Premium & Modicon Quantum:

## Schneider Electric Security Notification

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.

To mitigate the risks to Modicon Premium and Modicon Quantum controllers associated to this TCP protocol weakness, users should immediately:

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

### 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](http://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 to prevent unauthorized access to the ICS and safety controllers, peripheral equipment and 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 are 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.

## Schneider Electric Security Notification

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that these networks might have vulnerabilities and therefore 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-2019-6821	David Formby & Raheem Beyah of Fortify Logic and Georgia Tech

### 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.

# Schneider Electric Security Notification

## 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](http://www.schneider-electric.com)

## Revision Control:

<p><b>Version 1</b> <i>14 May 2019</i></p>	<p>Original Release</p>
--	-------------------------