

# Schneider Electric Security Notification

## Security Notification – Modicon Controllers (V3.0)

14 May 2019 (9 November 2021)

### Overview

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

**November 2021 Update:** Clarification of impacted commercial references: added BMENOP0300x, BMENOC03x1, BMENOS0300 and removed Modicon M340 CPU.

### Affected Products

Product	Version
Modicon M580	CPU firmware versions prior to V2.30 BMECRA* (EIO Drop adapter and) prior to V2.70 BMENOP0300x communication module prior to v2.5 BMENOC0301 communication module prior to v2.19 BMENOC0321 communication module prior to v1.07 BMENOS0300 network option switch prior to v1.02
Modicon RIO Drop adapters for M580, M340 and Quantum	BMECRA* (EIO Drop adapter and) prior to V2.70 BMXCRA* (RIO Drop adapter) prior to V2.70 140CRA (RIO Drop adapter) prior to V2.70 140CRA31908 (M580 Quantum S908 RIO Drop Adapter) prior to V2.70
Modicon Premium CPU and communication modules	all firmware versions
Modicon Quantum	140CPU* and communication modules - 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.

## Schneider Electric Security Notification

### Remediation

The most recent versions of the **Modicon M580 CPU** firmware (V2.30 and newer) fix this vulnerability. The latest version V3.20 is available for free download below.

M580 CPU V3.20 Firmware	
BMEx58x0x0	<a href="https://www.se.com/ww/en/download/document/BMEx58x0x0x_SV_xx.xx/">https://www.se.com/ww/en/download/document/BMEx58x0x0x_SV_xx.xx/</a>

#### Modicon M580 Communication modules:

Modicon communication modules Firmware	
BMENOP0300x v2.5	<a href="https://www.se.com/ww/en/download/document/BMENOP0300_Firmware_Update/">https://www.se.com/ww/en/download/document/BMENOP0300_Firmware_Update/</a>
BMENOC0301 v2.19	<a href="https://www.se.com/ww/en/download/document/BMENOC0301%20Exec%20and%20Release%20Notes/">https://www.se.com/ww/en/download/document/BMENOC0301%20Exec%20and%20Release%20Notes/</a>
BMENOC0311 v2.19	<a href="https://www.se.com/ww/en/download/document/BMENOC0311%20Exec%20and%20Release%20Notes/">https://www.se.com/ww/en/download/document/BMENOC0311%20Exec%20and%20Release%20Notes/</a>
BMENOC0321 v1.07	<a href="https://www.se.com/ww/en/download/document/BMENOC0321_Firmware/">https://www.se.com/ww/en/download/document/BMENOC0321_Firmware/</a>
BMENOS0300 v1.02	<a href="https://www.se.com/ww/en/download/document/BMENOS0300_Firmware/">https://www.se.com/ww/en/download/document/BMENOS0300_Firmware /</a>

#### Modicon RIO Drop Adapters:

The most recent versions of the BMX/BME/140 CRA (**RIO Drop Adapters**) firmware V2.70 and newer fix this vulnerability. The latest version V2.70 is available for free download below.

Modicon CRA (RIO Drop Adapters) V2.70:	
BMXCRA31200 BMXCRA31210 (C) BMECRA31210 (C) 140CRA31200 (C) 140CRA31908 (C)	<a href="https://www.se.com/ww/en/download/document/BMxCRA312x0_SV_xx.xx/">https://www.se.com/ww/en/download/document/BMxCRA312x0_SV_xx.xx/</a>

#### Modicon Premium & Modicon Quantum:

Schneider Electric's Modicon Quantum and Premium 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.

## Schneider Electric Security Notification

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.
- Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert.

### 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 the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

## Schneider Electric Security Notification

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

### Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher Names
CVE-2019-6821	David Formby & Raheem Beyah of Fortify Logic and Georgia Tech

### 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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: <https://www.se.com/ww/en/work/solutions/cybersecurity/>. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

#### LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

[www.se.com](http://www.se.com)

## Revision Control:

<b>Version 1.0</b> <i>14 May 2019</i>	Original Release
<b>Version 2.0</b> <i>08 June 2021</i>	Added a fix for CRA modules (RIO Drop Adapters) and a new mitigation option. ( <a href="#">page 2</a> )
<b>Version 3.0</b> <i>9 November 2021</i>	Added BMENOP0300x, BMENOC03x1, BMENOS0300 and removed Modicon M340 CPU from affected product list ( <a href="#">page 1</a> )