Schneider Electric Security Notification

Security Notification – Modicon Controllers (V2.0)

14 May 2019 (8 June 2021)

Overview

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

Update June 2021: Added a fix for CRA modules (RIO Drop Adapters) and a new mitigation option.

Affected Products

- Modicon M580
  - CPU firmware versions prior to V2.30
  - CRA (EIO Drop adapter and M580 Quantum S908 RIO Drop Adapter) prior to V2.70
- Modicon M340
  - CPU all firmware versions
  - CRA (RIO Drop adapter) prior to V2.70
- Modicon Premium - all firmware versions
- Modicon Quantum - all firmware versions
  - CRA (RIO Drop adapter) prior to V2.70

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 CPU** firmware (V2.30 and newer) fixes this vulnerability. The latest version V3.20 is available for free download below.

M580 CPU V3.20 Firmware	
BMEx58x0x0	https://www.se.com/ww/en/download/document/BMEx58x0x0x_SV_xx.xx/

Modicon RIO Drop Adapters:

The most recent versions of the BMX/BME 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)	https://www.se.com/ww/en/download/document/BMxCRA312x0_SV_xx.xx/

Schneider Electric is establishing a remediation plan for the future versions of 140CRA31200 and 140CRA31908 (Quantum CRA - RIO Drop Adapters) that will include a fix for this vulnerability. We will update this document when the remediation is available. Until then, customers should immediately apply the mitigations presented below, to reduce the risk of exploit.

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

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.

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

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.

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 Fortiphyd 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

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.

Schneider Electric Security Notification

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

Revision Control:

Version 1.0 *14 May 2019*	Original Release
Version 1.0 *8 June 2021*	Added a fix for CRA modules (RIO Drop Adapters) and a new mitigation option. (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.06.06 19:55:02 -04'00'