

Schneider Electric Security Notification

Modicon PAC Controllers

9 August 2022

Overview

Schneider Electric is aware of a vulnerability in its Modicon PAC Controllers.

[Modicon PLCs \(Programmable Logic Controllers\) and PACs \(Programmable Automation Controllers\)](#) control and monitor industrial operations in a sustainable, flexible, efficient, and protected way.

Failure to apply the remediations provided below may risk memory related errors, which could result in Denial of Service of the controller when using Modbus TCP.

Affected Products and Versions

Product	Version
Modicon M340 CPU (part numbers BMXP34*)	V3.40 and prior
Modicon M580 CPU (part numbers BMEP* and BMEH*)	V3.22 and prior
Legacy Modicon Quantum/Premium	All Versions
Modicon Momentum MDI (171CBU*)	All Versions
Modicon MC80 (BMKC80)	All Versions

Vulnerability Details

CVE ID: **CVE-2022-37301**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-191: Integer Underflow (Wrap or Wraparound)* vulnerability exists that could cause a denial of service of the controller due to memory access violations when using the Modbus TCP protocol.

Schneider Electric Security Notification

Remediation

Affected Products	Remediations
Modicon Modicon M340 CPU (part numbers BMXP34*) <i>V3.40 and prior</i>	Firmware V3.50 of Modicon includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_03.50/
Modicon M580 CPU (part numbers BMEP* and BMEH*) <i>V3.22 and prior</i>	Firmware V4.01 includes a fix for this vulnerability and is available for download here: https://www.se.com/us/en/product-range/62098-modicon-m580-pac-controller/#software-and-firmware
Modicon MC80 (BMKC80) <i>All Versions</i>	Schneider Electric is establishing a remediation plan for all future versions of Modicon MC80 and Modicon Momentum MDI that will include a fix for this vulnerability. We will update this document when the remediation is available.
Modicon MOMENTUM CPU (171CBU*) <i>All Versions</i>	
Legacy Modicon Quantum/Premium <i>All Versions</i>	Schneider Electric’s Modicon Premium and 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 They have been replaced by the Modicon M580 ePAC controller, our current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric’s [Customer Care Center](#) if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the mitigations provided in the table below.

Schneider Electric Security Notification

Affected Product	Mitigations
Modicon Modicon M340 CPU (part numbers BMXP34*) <i>V3.40 and prior</i>	<ul style="list-style-type: none"> • Setup an application password in the project properties • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure the Access Control List following the recommendations of the user manuals: <ul style="list-style-type: none"> ○ “Modicon M580, Hardware, Reference Manual” https://www.se.com/ww/en/download/document/EIO00000001578/ ○ “Modicon M340 for Ethernet Communications Modules and Processors User Manual” in chapter “Messaging Configuration Parameters”: https://www.se.com/ww/en/download/document/31007131K01000/ ○ “Modicon MC80 Programmable Logic Controller (PLC) manual” in the chapter “Access Control List (ACL)” https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000002071.02.pdf&p_Doc_Ref=EIO0000002071 ○ “Momentum for EcoStruxure™ Control Expert - 171 CBU 78090, 171 CBU 98090, 171 CBU 98091 Processors” manual in the chapter “Modbus Messaging and Access Control” https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=HRB44124.08.pdf&p_Doc_Ref=HRB44124 • Setup a secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual,” in chapter “Setup secured communications”: https://www.se.com/ww/en/download/document/EIO0000001999/
Modicon M580 CPU (part numbers BMEP* and BMEH*) <i>V3.22 and prior</i>	
Modicon MC80 (BMKC80) <i>All Versions</i>	

Schneider Electric Security Notification

<p>Modicon MOMENTUM CPU (171CBU*) <i>All Versions</i></p>	<ul style="list-style-type: none"> • Use a BMENOC module and follow the instructions to configure IPSEC feature as described in the guideline “Modicon M580 - BMENOC03.1 Ethernet Communications Schneider Electric Security Notification Module, Installation and Configuration Guide” in the chapter “Configuring IPSEC communications”: https://www.se.com/ww/en/download/document/HRB62665/ • Setup a VPN between the Modicon PLC controllers and the engineering workstation containing EcoStruxure Control Expert or Process Expert. Note: this functionality may be provided by an external IPSEC compatible firewall located close to the controller. <p>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric’s security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp</p>
<p>Legacy Modicon Quantum/Premium <i>All Versions</i></p>	<p>If customers choose not to upgrade, they should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure the Access Control List feature as mentioned in “Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual” in chapter “Software Settings for Ethernet Communication / Messaging / Quantum NOE Ethernet Messaging Configuration”: https://www.se.com/ww/en/download/document/33002467K01000/ • Configure the Access Control List following the recommendations of the user manual “Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual” in chapters “Connection configuration parameters / TCP/IP Services Configuration Parameters / Connection Configuration Parameters”: https://www.se.com/ww/en/download/document/35006192K01000/

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric’s security notification service here:

<https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp>

Schneider Electric Security Notification

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 intended for that device.
- 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 researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2022-37301	Li WEI, BooleanTech

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.

Schneider Electric Security Notification

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

About Schneider Electric

Schneider’s purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Revision Control:

Version 1.0 09-Aug-22	Original Release
---------------------------------	------------------