Life Is On | Schneider Electric

Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert and Modicon M340, M580 and M580 CPU Safety

10 January 2023 (9 January 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Control Expert, EcoStruxure™ Process Expert, Modicon M340, M580 and M580 CPU Safety.

The Modicon M580 are PAC and Safety PLCs with built-in Ethernet for process, high availability & safety solutions.

The Modicon M340 offers compactness, flexibility, scalability, and robustness for the process industry and a wide range of demanding automation applications.

EcoStruxure™ Control Expert is the common programming, debugging and operating software for Modicon PLCs (Programmable Logic Controllers) and PACs (Programmable Automation Controllers).

The EcoStruxure™ Process Expert DCS is a single automation system to engineer, operate, and maintain your entire infrastructure for a sustainable, productive and market-agile plant.

Failure to apply the mitigations provided below may risk unauthorized access to your PLC, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.

January 2024 Update: A remediation is available on Modicon M580 (page 2).

Affected Products and Versions

Product	Version
EcoStruxure™ Control Expert	All versions
EcoStruxure™ Process Expert	All versions
Modicon M340 CPU (part numbers BMXP34*)	All versions
Modicon M580 CPU (part numbers BMEP* and BMEH*)	Versions prior to sv4.20
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)	All versions
Modicon Momentum Unity M1E Processor (171CBU*)	All versions
Modicon MC80 (BMKC80)	All versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2022-45789**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-294: Authentication Bypass by Capture-replay* vulnerability exists that could cause execution of unauthorized Modbus functions on the controller when hijacking an authenticated Modbus session.

Remediation

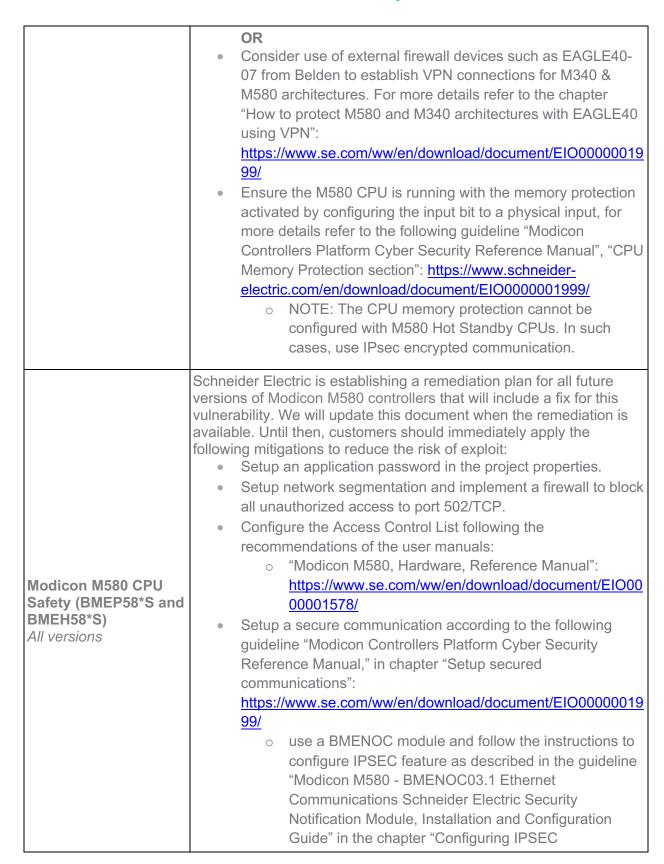| Affected Product & Version	Remediation
Modicon M580 (part numbers BMEP* and BMEH*, excluding M580 CPU Safety) *Versions prior to sv4.20*	Firmware sv4.20 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/62098-modicon-m580-epac/#software-and-firmware

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.

Schneider Electric Security Notification

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Control Expert *All versions*	Schneider Electric is establishing a remediation plan for all future versions of EcoStruxure™ Control Expert 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 following mitigations to reduce the risk of exploit: • Setup a VPN between the Modicon PLC controllers and the engineering workstation containing EcoStruxure™ Control Expert. Note: this functionality may be provided by an external IPSEC compatible firewall located close to the controller. • Harden the workstation running EcoStruxure™ Control Expert.
EcoStruxure™ Process Expert *All versions*	Schneider Electric is establishing a remediation plan for all future versions of EcoStruxure™ Process Expert 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 following mitigations to reduce the risk of exploit: • Setup a VPN between the Modicon PLC controllers and the engineering workstation containing EcoStruxure™ Process Expert. Note: this functionality may be provided by an external IPSEC compatible firewall located close to the controller. • Harden the workstation running EcoStruxure™ Process Expert.
Modicon M340 CPU (part numbers BMXP34*) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of M340 Controllers 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 following mitigations to reduce the risk of exploit: • 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: o "Modicon M340 for Ethernet Communications Modules and Processors User Manual" in chapter "Messaging Configuration Parameters": https://www.se.com/ww/en/download/document/31007131K01000/ • 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/EIO00000019 99/ • Consider the use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections for M340 & M580 architectures. For more details refer to the chapter "How to protect M580 and M340 architectures with EAGLE40 using VPN": https://www.se.com/ww/en/download/document/EIO00000019 99/

Modicon M580 CPU (part numbers BMEP* and BMEH*)
Versions prior to sv4.20
	If customers choose not to apply the remediation, it is recommended to apply the following mitigations to reduce the risk of the exploit:
	• 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:
	  o "Modicon M580, Hardware, Reference Manual":
	    https://www.se.com/ww/en/download/document/EIO00
	    00001578/
	• 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/EIO00000019
	99/
	  o 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/HRB6
	    2665/
	
	  OR
	• Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter "Configuring the BMENUA0100 Cybersecurity Settings":
	https://www.se.com/ww/en/download/document/PHA83350

	OR • Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections for M340 & M580 architectures. For more details refer to the chapter "How to protect M580 and M340 architectures with EAGLE40 using VPN": https://www.se.com/ww/en/download/document/EIO0000001999/ • Ensure the M580 CPU is running with the memory protection activated by configuring the input bit to a physical input, for more details refer to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual", "CPU Memory Protection section": https://www.schneider-electric.com/en/download/document/EIO0000001999/ ○ NOTE: The CPU memory protection cannot be configured with M580 Hot Standby CPUs. In such cases, use IPsec encrypted communication.

Modicon M580 CPU Safety (BMEP58*S and BMEH58*S)
All versions
	Schneider Electric is establishing a remediation plan for all future versions of Modicon M580 controllers 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 following mitigations to reduce the risk of exploit:
	• 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:
	    ○ "Modicon M580, Hardware, Reference Manual": https://www.se.com/ww/en/download/document/EIO0000001578/
	• 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/
	    ○ 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/

OR

- Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter "Configuring the BMENUA0100 Cybersecurity Settings": https://www.se.com/ww/en/download/document/PHA83350

OR

- Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections for M340 & M580 architectures. For more details refer to the chapter "How to protect M580 and M340 architectures with EAGLE40 using VPN": https://www.se.com/ww/en/download/document/EIO0000001999/

- Ensure the M580 CPU is running with the memory protection activated by configuring the input bit to a physical input, for more details refer to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual", "CPU Memory Protection section": https://www.schneider-electric.com/en/download/document/EIO0000001999/
  - NOTE: The CPU memory protection cannot be configured with M580 Hot Standby CPUs. In such cases, use IPsec encrypted communication.

To further reduce the attack surface on Modicon M580 CPU Safety:
  - Ensure the CPU is running in Safety mode and maintenance input is configured to maintain this Safety mode during operation – refer to the document Modicon M580 - Safety System Planning Guide - in the chapter "Operating Mode Transitions": https://www.se.com/ww/en/download/document/QGH60283/

Schneider Electric Security Notification

Modicon MOMENTUM Unity M1E Processor (part numbers 171CBU*) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon MOMENTUM Unity M1E controllers 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 following mitigations to reduce the risk of exploit:
	
	• 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:
	
	    • "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://www.se.com/ww/en/download/document/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 MC80 (part numbers BMKC80) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon MC80 controllers 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 following mitigations to reduce the risk of exploit:
	
	• 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:
	
	    • "Modicon MC80 Programmable Logic Controller (PLC) manual" in the chapter "Access Control List (ACL)": https://www.se.com/ww/en/download/document/EIO0000002071/
	    • 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/

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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2022-45789	Jos Wetzels and Daniel dos Santos, Forescout Technologies

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

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 1.0.0 10 January 2023	Original Release
Version 2.0.0 14 March 2023	Modicon Momentum Unity M1E Process and Modicon MC80 were added to the impacted products with the mitigations.

Version 3.00.0 *08 August 2023*	All versions of the EcoStruxure™ Process Expert are impacted by this vulnerability ([page 3](#)).
Version 4.0.0 *09 January 2024*	A remediation is available for Modicon M580 ([page 2](#)).