Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert, and Modicon Controllers M580 and M340

9 August 2022 (13 December 2022)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Control Expert , EcoStruxure™ Process Expert, and Modicon M580 and M340 control products.
Failure to apply the remediations provided below may risk a bypass of access controls in place, which could result in the possibility of arbitrary code execution and loss of confidentiality and integrity of the project file.

December 2022 Update: The Modicon M580 SV4.02 firmware has been retracted for quality issues and is no longer available for download. Additional mitigations have been introduced for Modicon M580 CPU (page 2) and M580 CPU Safety (page 3), and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.

Affected Products and Versions

Product	Version
EcoStruxure™ Control Expert Including all Unity Pro versions (former name of EcoStruxure™ Control Expert)	V15.0 SP1 and prior
EcoStruxure™ Process Expert, Including all versions of EcoStruxure™ Hybrid DCS (former name of EcoStruxure™ Process Expert)	Prior to V2021
Modicon M340 CPU (part numbers BMXP34*)	V3.40 and prior
Modicon M580 CPU (part numbers BMEP* and BMEH*)	V3.20 and prior
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)	All Versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2022-37300**
CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
A *CWE-640: Weak Password Recovery Mechanism for Forgotten Password* vulnerability exists that could cause unauthorized access in read and write mode to the controller when communicating over Modbus.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Control Expert Including all Unity Pro versions (former name of EcoStruxure™ Control Expert) *Versions prior V15.1*	EcoStruxure Control Expert V15.1, available for download below, includes a fix for this vulnerability: https://www.se.com/us/en/product-range/548-ecostruxure-control-expert-software/ - software-and-firmware
EcoStruxure™ Process Expert, Including all versions of EcoStruxure™ Hybrid DCS (former name of EcoStruxure™ Process Expert) *Versions prior to V2021*	EcoStruxure™ Process Expert V2021, available for download below, includes a fix for this vulnerability: https://www.se.com/ww/en/product-range/65406-ecostruxure-process-expert/ - software-and-firmware
Modicon M340 CPU (part numbers BMXP34*) *Versions prior to V3.50*	Firmware V3.50 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*) *All Versions*	The Modicon M580 SV4.02 firmware has been retracted for quality issues and is no longer available for download. For specific questions or support, Customers are requested to contact Schneider Electric's Customer Care Center Please refer to the mitigations recommended in the section below.

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 available in the mitigation section below.

Affected Product	Mitigations

Modicon Modicon M340 CPU (part numbers BMXP34*) *Versions prior to V3.50*	• 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/
	  ○ "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/EIO0000001999/
	• 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
	• 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/
	• 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.

Modicon M580 CPU (part numbers BMEP* and BMEH*) *All Versions*	
Modicon M580 CPU Safety (BMEP58*S and BMEH58*S) *All Versions*	

	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 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/
EcoStruxure™ Control Expert *Versions prior to V15.1*	• 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. • Store the project files in a secure storage and restrict the access to only trusted users • When exchanging files over the network, use secure communication protocols • Encrypt project files when stored • Only open project files received from trusted source • Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage • Harden the workstation running EcoStruxure™ Control Expert and EcoStruxure™ Process Expert
EcoStruxure™ Process Expert *Versions prior to V2021*	

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-2022-37300	GAO Jin (NSFocus)

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

Schneider Electric Security Notification

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 August 2022*	Original Release
Version 1.1 *06 September 2022*	The version number for Modicon M580 that addresses these vulnerabilities has been updated from SV4.01 to SV4.02.
Version 2.0 *11 October 2022*	A clarification was added to the list of affected products by splitting Modicon M580 and Modicon M580 Safety CPU ranges. The purpose of the notification update is to inform customers that the latest fix Modicon M580 SV4.02 does not apply to the Safety range of M580. It is highly recommended that customers using Modicon M580 Safety ranges continue to implement the mitigations shared in this document.
Version 3.0 *13 December 2022*	The Modicon M580 SV4.02 firmware has been retracted for quality issues and is no longer available for download. Additional mitigations have been introduced for Modicon M580 CPU (page 2) and M580 CPU Safety (page 3), and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.

Product Security Office

Digitally signed by Product Security Office
Date: 2022.12.12 14:28:47 -05'00'