Schneider Electric Security Notification

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

13 February 2024 (13 August 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Control Expert , EcoStruxure™ Process Expert and Modicon M340, M580 PLCs (Programmable Logic Controllers).

Modicon PLCs control and monitor industrial operations. EcoStruxure™ Control Expert is the common programming, debugging and operating software for Modicon PLCs. EcoStruxure™ Process Expert DCS is a single automation system to engineer, operate, and maintain an entire plant Infrastructure.

Failure to apply the remediations 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.

August 2024 Update: A remediation is available for the Modicon M580 CPU Safety (page 3).

Affected Products and Versions

Product	Version	CVE-2023-27975	CVE-2023-6408	CVE-2023-6409
Modicon M340 CPU (part numbers BMXP34*)	Versions prior to SV3.60		x	
Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety)	Versions prior to SV4.20		x	
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)	Versions prior to SV4.21		x	
Modicon MC80 (part numbers BMKC80)	All versions		x	
Modicon Momentum Unity M1E Processor (171CBU*)	All versions		x	
EcoStruxure™ Control Expert	Versions prior to v16.0	x	x	x
EcoStruxure™ Process Expert	Versions prior to v2023	x	x	x

Vulnerability Details

CVE ID: **CVE-2023-6408**

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

CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause a denial of service and loss of confidentiality, integrity of controllers when conducting a Man in the Middle attack.

CVE ID: **CVE-2023-6409**

CVSS v3.1 Base Score 7.7 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CWE-798: Use of Hard-coded Credentials vulnerability exists that could cause unauthorized access to a project file protected with application password when opening the file with EcoStruxure Control Expert.

CVE ID: **CVE-2023-27975**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause unauthorized access to the project file in EcoStruxure™ Control Expert when a local user tampers with the memory of the engineering workstation.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

Affected Product & Version	Remediation	CVE
Modicon M340 CPU (part numbers BMXP34*) *Versions prior to SV3.60*	SV3.60 of Modicon M340 firmware includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/1468-modicon-m340	CVE-2023-6408
Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety) *Versions prior to SV4.20*	SV4.20 of Modicon M580 firmware 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	
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S) *Versions prior to SV4.21*	Firmware SV4.21 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/62098-modicon-m580-pac-controller/#software-and-firmware Important: customer needs to use version of EcoStruxure™ Control Expert v16.0 HF001 minimum to connect with the latest version of M580 CPU Safety. The software is available for download here: https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware	CVE-2023-6408
EcoStruxure™ Control Expert *Versions prior to v16.0*	Version 16.0 of EcoStruxure™ Control Expert includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/ Reboot the computer after installation is completed.	CVE-2023-27975 CVE-2023-6408 CVE-2023-6409
EcoStruxure™ Process Expert *Versions prior to v2023*	Version 15.3 HF008 of EcoStruxure™ Control Expert includes the fix for these vulnerabilities and are available for download here: https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/	CVE-2023-27975 CVE-2023-6408 CVE-2023-6409

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 following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
Modicon M340 CPU (part numbers BMXP34*) *Versions prior to SV3.60*	• 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 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/ • 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 M340 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.se.com/ww/en/download/document/EIO0000001999/
Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety) *Versions prior to SV4.20*	• 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.
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S) *Versions prior to SV4.21*	• 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/
Modicon MC80 (part numbers BMKC80) *All versions*	• 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 Controller Systems Cybersecurity, User Guide” in chapter “Set Up Encrypted Communication”: https://www.se.com/ww/en/download/document/EIO0000001999/
Modicon Momentum Unity M1E Processor (part numbers 171CBU*) *All versions*	• Setup an application password in the project properties • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP Setup a secure communication according to the following guideline “Modicon Controller Systems Cybersecurity, User Guide” in chapter “Set Up Encrypted Communication”: https://www.se.com/ww/en/download/document/EIO0000001999/
EcoStruxure™ Control Expert *Versions prior to v16.0*	• Enable encryption on application project and store application files in secure location with restricted access only for legitimate users. • Schneider Electric recommends using McAfee Application and Change Control software for application control. Refer to the Cybersecurity Application Note available here. • Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices available for download here.
EcoStruxure™ Process Expert *Versions prior to v2023*	• EcoStruxure Process Expert manages application files within its database in secure way. Do not export & store them outside the application. • Schneider Electric recommends using McAfee Application and Change Control software for application control. Refer to the Cybersecurity Application Note available here.

	- Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices available for download here.

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

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 these vulnerabilities:

CVE	Researchers
CVE-2023-6408	Gao Jian

CVE-2023-6409	Jianshuang Ding
CVE-2023-27975	Kaikai Yang

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.

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.

Schneider Electric Security Notification

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 *13 February 2024*	Original Release
Version 2.0.0 *09 July 2024*	Modicon MC80 and Momentum M1E PLCs have been identified as impacted by the CVE-2023-6408. Mitigations are now available.
Version 3.0.0 *13 August 2024*	A remediation is available for the Modicon M580 CPU Safety (page 3).