Life Is On Schneider Electric

Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert and Modicon PLCs and PACs

10 January 2023 (8 August 2023)

Overview

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

Modicon PLCs and PACs control and monitor industrial operations. EcoStruxure™ Control Expert is the common programming, debugging and operating software for Modicon PLCs and PACs. 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 2023 Update: All versions of the EcoStruxure™ Process Expert are impacted by this vulnerability (page 3).

Affected Products and Versions

Product	Version
EcoStruxure™ Control Expert	Versions prior to V15.3
EcoStruxure™ Process Expert	All Versions
Modicon M340 CPU (part numbers BMXP34*)	Version prior to SV3.51
Modicon M580 CPU (part numbers BMEP* and BMEH*)	Versions prior to SV4.10
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S)	All Versions
Modicon Momentum Unity M1E Processor (171CBU*)	Versions prior to SV2.6
Modicon MC80 (BMKC80*)	Versions prior to SV1.90
Legacy Modicon Quantum (140CPU65*) and Premium CPUs (TSXP57*)	All Versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2022-45788**

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

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists that could cause arbitrary code execution, denial of service and loss of confidentiality & integrity when a malicious project file is loaded onto the controller.

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
EcoStruxure™ Control Expert *Versions prior to v15.3*	Software v15.3 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/EcoStruxureControlExpert-V15.3/
Modicon M580 (part numbers BMEP* and BMEH*, excluding M580 CPU Safety) *Versions prior to SV4.10*	Firmware SV4.10 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMEx58x0x0_SV04.10/
Modicon Momentum Unity M1E Processor (part numbers 171CBU*) *Versions prior to VS2.6*	Firmware SV2.6 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/Momentum_FW_update/
Modicon Modicon M340 CPU (part numbers BMXP34*) *Versions prior to SV3.51*	Firmware SV3.51 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/1468-modicon-m340/#software-and-firmware
Modicon MC80 CPU (part numbers BMKC80*) *Versions prior to SV1.90*	Firmware SV1.90 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMKC80_Firmware_upgrade/

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.

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Control Expert *Versions prior to v15.3*	If customers choose not to apply the remediation, it is recommended to apply the following mitigations to reduce the risk of the 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. • It is recommended to enable the file encryption feature for all new projects. • Encrypt project files when stored and restrict the access to only trusted users. • When exchanging files over the network, use secure communication protocols. • Only open project files received from a trusted source, and it is recommended to share project files only when configured with the encryption feature described above. Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage.
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. • Encrypt project files when stored and restrict the access to only trusted users. • When exchanging files over the network, use secure communication protocols. • 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™ Process Expert.
Modicon Modicon M340 CPU (part numbers BMXP34*)	If customers choose not to apply the remediation, it is recommended to apply the following mitigations to reduce the risk of the exploit:

Versions prior to SV3.51	• 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.schneider-electric.com/en/download/document/EIO0000001999/
Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety) *Versions prior to v4.10*	If customers choose not to apply the remediation, then they 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.
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 Safety 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/

Modicon MOMENTUM Unity M1E Processor(171CBU*) *Versions prior to SV2.6*	If customers choose not to apply the remediation, then they 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 (BMKC80) *All versions prior to SV1.90*	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: • "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/
Modicon Premium CPU (TSXP5*) **& Quantum CPU** (140CPU65*) *All versions*	Schneider Electric's Modicon Premium & 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 most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

	To mitigate the risks users should immediately: • 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 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/

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-2022-45788	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.

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.

Schneider Electric Security Notification

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 *10 January 2023*	Original Release
Version 2.0 *14 March 2023*	Remediation for EcoStruxure™ Control Expert, Modicon M580 CPU, and Momentum Unity M1E Processor are available for download (page 2). Additional mitigations for Modicon M340 were added.
Version 3.0 *11 April 2023*	Remediation for M340 was added in the remediation section (page 2). Qualitative severity rating was corrected to “high” to reflect the CVSS score.
Version 4.0 *11 July 2023*	Remediation for MC80 is added in the remediation section (page 3)
Version 5.0 *8 August 2023*	All versions of the EcoStruxure™ Process Expert are impacted by this vulnerability (page 3).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.08.07 14:13:09 -04'00'