Schneider Electric Security Notification

Modicon PAC Controllers and PLC Simulator for EcoStruxure™ Control Expert and EcoStruxure™ Process Expert

10 August 2021 (11 July 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities in the Modicon PAC Controllers and PLC simulator included in EcoStruxure™ Control Expert and EcoStruxure™ Process Expert.

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

The PLC Simulator feature is part of the EcoStruxure™ Control Expert and EcoStruxure™ Process Expert software and it helps users to review and test their configurations files in a simulation environment and is not intended to be used as a controller CPU in a production environment.

Failure to apply the mitigations provided below may lead to the execution of a malicious project file, which could result in loss of availability of the controller or of the PLC simulator. For an attack to be successful, a malicious project file must be downloaded in the controller or in the simulator.

July 2023 Update: A remediation is available for Modicon MC80 (page 3).

Affected Products and Versions

Product	CVE-2021-22789	CVE-2021-22790	CVE-2021-22791	CVE-2021-22792
Modicon M580 CPU (part numbers BMEP* and BMEH*, excluding M580 CPU Safety), Versions prior to SV4.10	X	x	x	x
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S), All Versions	X	x	x	x
Modicon M340 CPU (part numbers BMXP34*), All versions prior to V3.50	X	x	x	x
Modicon MC80 (part numbers BMKC80*), All versions prior to SV1.90	X			
Modicon Momentum Unity M1E Processor (part numbers 171CBU*), Versions prior to SV2.6	X			
PLC Simulator for EcoStruxure™ Control Expert *Including all Unity Pro versions (former name of EcoStruxure™ Control Expert)*, All Versions	x	x	x	x
PLC Simulator for EcoStruxure™ Process Expert *including all HDCS versions (former name of EcoStruxure™ Process Expert)*, All Versions	x	x	x	x
Legacy Modicon Premium and Quantum, All Versions	X	x	x	x

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2021-22789**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer* vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.

CVE ID: **CVE-2021-22790**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-125: Out-of-Bounds Read* vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.

CVE ID: **CVE-2021-22791**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-787: Out-of-Bounds Write* vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.

CVE ID: **CVE-2021-22792**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-476: NULL Pointer Dereference* vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.

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 & Final Mitigations

Affected Product & Version	Remediation
Modicon M340 CPU (part numbers BMXP34*) *All versions prior to V3.50*	M340 V3.50 includes a fix for these vulnerabilities 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*, excluding M580 CPU Safety) *All versions prior to SV4.10*	Modicon M580 SV4.10 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMEx58x0x0_SV04.10/
Modicon MC80 (BMKC80) *All versions prior to SV1.90*	Firmware SV1.90 includes a fix for CVE-2021-22789 vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMKC80_Firmware_upgrade/
Modicon MOMENTUM CPU (171CBU*) *Versions prior to SV2.6*	Firmware SV2.6 includes a fix for CVE-2021-22789 vulnerability and is available for download here: https://www.se.com/ww/en/download/document/Momentum_FW_update/
Legacy Modicon Quantum/Premium *All versions*	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.

PLC Simulator for EcoStruxure™ Control Expert including all Unity Pro versions (former name of EcoStruxure™ Control Expert)
All versions
	Customers should immediately apply the following mitigations to reduce the risk of exploit:
	• Download and setup EcoStruxure Control Expert V15.0 SP1 from this link: https://www.se.com/ww/en/download/document/EcoStruxureControlExpert_15SP1
	  ○ Use the new "file encryption" feature available on EcoStruxure Control Expert v15.0 SP1 in order to protect the project files.
	  ○ Ensure to use simulator default panel option to make PLC simulator accessible only locally.
	• 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 or Unity Pro
	
	Note: The PLC Simulator feature is part of the EcoStruxure Control Expert and EcoStruxure Process Expert software, and it helps users to review and test their configurations files in a simulation environment. It is not intended to be used as a controller CPU in a production environment.
	
	Update: Refer to the PLC Simulator user manual for more details on enforcing security settings available here.

PLC Simulator for EcoStruxure™ Process Expert including all HDCS versions (former name of EcoStruxure™ Process Expert) *All versions*	Customers should immediately apply the following mitigations to reduce the risk of exploit: • 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 or Unity Pro

	Note: The PLC Simulator feature is part of the EcoStruxure Control Expert and EcoStruxure Process Expert software, and it helps users to review and test their configurations files in a simulation environment. It is not intended to be used as a controller CPU in a production environment. **Update: Refer to the PLC Simulator user manual for more details on enforcing security settings available here.**
Modicon Premium CPU (part numbers TSXP5*) *All versions*	Schneider Electric's Modicon Premium 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/

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.

Mitigations

Affected Product	Mitigations
Modicon M340 CPU (part numbers BMXP34*) *All 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/ ○ "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 ○ 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 • Setup a VPN between the Modicon PLC controller 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. 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
Modicon M580 CPU (part numbers BMEP* and BMEH* excluding M580 CPU Safety) *All versions prior to V4.10*	
Modicon M580 CPU Safety (part numbers BMEP58*S and BMEH58*S) *All versions*	
Modicon MOMENTUM Unity M1E Processor(171CBU) *Versions prior to V2.6*	
Modicon MC80 (BMKC80*) *All versions prior to SV1.90*	

Modicon Premium CPU (part numbers TSXP5*) All versions	Schneider Electric's Modicon Premium 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/

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 for the devices that it is intended for.
- 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.

Schneider Electric Security Notification

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-2021-22789	Kai Wang (Codesafe Team of Legendsec at Qi'anxin Group) Guillaume Orlando (Airbus Cybersecurity)
CVE-2021-22790 CVE-2021-22791 CVE-2021-22792	Kai Wang (Codesafe Team of Legendsec at Qi'anxin Group)

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

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 *10 August 2021*	Original Release
Version 2.0 *09 August 2022*	A fix is available for Modicon M340 and Modicon M580 that addresses these vulnerabilities.
Version 2.1 *06 September 2022*	The version number for Modicon M580 that addresses these vulnerabilities has been updated from V4.01 to V4.02.
Version 3.0 *11 October 2022*	A clarification 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 V4.02 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 (page 6).
Version 4.0 *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 and M580

	CPU Safety, and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.
Version 5.0 *14 March 2023*	A remediation is available for Modicon M580 CPU and Modicon Momentum Unity M1E Processor for CVE-2021-22789 (page 3), and update to the PLC Simulator user manual to reflect the mitigation (page 6).
Version 6.0 *11 July 2023*	A remediation is available for Modicon MC80 (page 3).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.09.11 09:41:13 -04'00'