Schneider Electric Security Notification

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

10 August 2021

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.

Affected Products and Versions

Product	Version
Modicon M580 CPU (part numbers BMEP* and BMEH*)	All versions
Modicon M340 CPU (part numbers BMXP34*)	All versions
Modicon MC80 (part numbers BMKC80*)	All versions
Modicon Momentum Ethernet CPU (part numbers 171CBU*)	All versions
PLC Simulator for EcoStruxure™ Control Expert *Including all Unity Pro versions (former name of EcoStruxure™ Control Expert)*	All versions
PLC Simulator for EcoStruxure™ Process Expert *including all HDCS versions (former name of EcoStruxure™ Process Expert)*	All versions
Modicon Quantum CPU (part numbers 140CPU*)	All versions
Modicon Premium CPU (part numbers TSXP5*)	All versions

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.

Mitigations

Schneider Electric encourages all industrial companies to ensure they have implemented cybersecurity best practices across their operations and supply chains to reduce cyber risks. Where appropriate this includes locating industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission critical systems and devices from being accessed from outside networks; systematically applying security patches. Additional recommended actions for the impacted products and listed below:

Affected Product	Mitigations
Modicon M580 CPU (part numbers BMEP* and BMEH*) All versions	Schneider Electric is establishing a remediation plan for the future versions of the Modicon M580 CPU. We will update this document when this will be available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup the application password found in the project properties section • 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 “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/ • Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert or Process Expert. 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

Schneider Electric Security Notification

Modicon M340 CPU (part numbers BMXP34*)
 	
All versions
 	
Modicon MC80 (part numbers BMKC80*)
 	
All versions
 	
Modicon Momentum Ethernet CPU (part numbers 171CBU*)
 	
All versions
	Schneider Electric is establishing a remediation plan for the future versions of M340 CPU, MC80, and Momentum Ethernet CPU. We will update this document when this will be 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 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
	• Setup a VPN between the Modicon PLC impacted modules 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

PLC Simulator for EcoStruxure™ Control Expert
 	
All versions including all Unity Pro versions (former name of EcoStruxure™ Control Expert)
	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
	• Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert.
	
	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.

PLC Simulator for EcoStruxure™ Process Expert All versions including all HDCS versions (former name of EcoStruxure™ Process Expert)	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 • Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert. 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.

Schneider Electric Security Notification

Modicon Quantum CPU (part numbers 140CPU*) All versions	Schneider Electric's Modicon 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 associated to Modbus/ weaknesses, users should immediately: • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure the Access Control List feature as mentioned in "Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual" in chapter "Software Settings for Ethernet Communication / Messaging / Quantum NOE Ethernet Messaging Configuration": https://www.se.com/ww/en/download/document/33002467K01000/
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/

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.

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-2021-22789 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

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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *10 August 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:03:58 -04'00'