Schneider Electric Security Notification

Modicon Controllers M340 / Momentum / MC80

12 November 2024

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 products.

Modicon PAC products control and monitor industrial operations.

Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controller, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.

Affected Products and Versions

Products	CVE-2024-8933	CVE-2024-8935
Modicon M340 CPU (part numbers BMXP34*)	All versions	All versions since SV3.60
Modicon MC80 (part numbers BMKC80)	All versions	Not impacted
Modicon Momentum Unity M1E Processor (171CBU*)	All versions	Not impacted

Vulnerability Details

CVE ID: **CVE-2024-8933**

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
CVSS v4.0 Base Score 7.5 | High | CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause retrieval of password hash that could lead to denial of service and loss of confidentiality and integrity of controllers. To be successful, the attacker needs to inject themself inside the logical network while a valid user uploads or downloads a project file into the controller.

CVE ID: **CVE-2024-8935**

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
CVSS v4.0 Base Score 7.7 | High | CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-290: Authentication Bypass by Spoofing vulnerability exists that could cause a denial of service and loss of confidentiality and integrity of controllers when conducting a Man-In-The-Middle attack between the controller and the engineering workstation while a valid user is establishing a communication session. This vulnerability is inherent to Diffie Hellman algorithm which does not protect against Man-In-The-Middle attacks.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 (CVSS v4.0). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated 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.

Mitigations

Affected Product & Version	Mitigations
Modicon M340 CPU (part numbers BMXP34*) *CVE-2024-8933: All versions* *CVE-2024-8935: Versions since SV3.60*	Schneider Electric is establishing a remediation plan for all future versions of Modicon M340 that will include a fix for CVE-2024-8933 vulnerability and a mitigation for CVE-2024-8935. 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 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/ • Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections. For more details refer to "Modicon Controller Systems Cybersecurity, User Guide": 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 Controller Systems Cybersecurity, User Guide" chapter "Controler Memory Protection": https://www.se.com/ww/en/download/document/EIO0000001999/
Modicon MC80 (part numbers BMKC80) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon MC80 that will include a fix for CVE-2024-8933. 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 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: "MC80 Programmable Logic Controller(PLC), User Manual" in the section "Access Control List (ACL)": https://www.se.com/ww/en/download/document/EIO0000002071/

	• Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections. For more details refer to "Modicon Controller Systems Cybersecurity, User Guide": https://www.se.com/ww/en/download/document/EIO0000001999/
Modicon Momentum Unity M1E Processor (171CBU*) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon Momentum that will include a fix for CVE-2024-8933. 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 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 - 171CBU78090, 171CBU98090, 171CBU98091 Processors, User Guide" in the section "Controlling Access": https://www.se.com/ww/en/download/document/HRB44124/ • Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections. For more details refer to "Modicon Controller Systems Cybersecurity, User Guide": -https://www.se.com/ww/en/download/document/EIO0000001999/

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-2024-8933	Artem Zinenko (Kaspersky) Amir Zaltzman (Tel Aviv University)
CVE-2024-8935	Amir Zaltzman (Tel Aviv University)

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.

Schneider Electric Security Notification

About Schneider Electric

Schneider's purpose is to **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency.**

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers.**

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 12 November 2024	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.11.11 09:06:10 -05'00'