Schneider Electric Security Notification

Ethernet and Web server on Modicon M340 controller and Communication Modules

11 January 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon M340 controller and Communication Modules.

The Modicon Ethernet Programmable Automation products are controllers for industrial process and infrastructure.

The Modicon M340 offers compactness, flexibility, scalability, and robustness for the process industry and a wide range of demanding automation applications. The Eagle40 device and the accompanying security guidance are intended to be the full solution for these vulnerabilities.

Failure to apply the mitigations provided below may risk disclosure of sensitive information, unauthorized web server actions and denial of service.

Affected Products and Versions

Product	Version	CVE
Modicon M340 CPUs: BMXP34*	All versions	CVE-2022-22724 CVE-2020-7534
Modicon Quantum CPUs with integrated Ethernet (Copro): 140CPU65*	All versions	CVE-2020-7534
Modicon Premium CPUs with integrated Ethernet (Copro): TSXP57*		
Modicon M340 ethernet modules: • BMXNOC0401 • BMXNOE01* • BMXNOR0200H	All versions	CVE-2020-7534
Modicon Quantum and Premium factory cast communication modules: • 140NOE77111 • 140NOC78*00 • TSXETY5103 • TSXETY4103	All versions	CVE-2020-7534

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2022-22724**

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

A *CWE-400: Uncontrolled Resource Consumption* vulnerability exists that could cause a denial of service on ports 80 (HTTP) and 502 (Modbus), when sending a large number of TCP RST or FIN packets to any open TCP port of the PLC.

CVE ID: **CVE-2020-7534**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H

A *CWE-352: Cross-Site Request Forgery (CSRF)* vulnerability exists on the web server used, that could cause a leak of sensitive data or unauthorized actions on the web server during the time the user is logged in.

Mitigations

Affected Product & Version	Mitigations
Modicon M340 CPUs: BMXP34* *All versions* Modicon Quantum CPUs with integrated Ethernet (Copro): 140CPU65* *All versions* Modicon Premium CPUs with integrated Ethernet (Copro): TSXP57* *All versions*	Customers should immediately apply the following mitigations to reduce the risk of exploit. For further details please check the Cyber Security Reference Manual available here: Modicon Controllers Platform - Cyber Security, Reference Manual User guide | Schneider Electric • Setup a VPN between the Modicon PLC modules and the engineering workstation containing EcoStruxure Control Expert or EcoStruxure Process Expert. For the **M340 offer**, the recommended configuration is described in the section "**How to protect M340 architectures with EAGLE40 using a VPN**" of the EcoStruxure Control Expert online help. • Configure the Access Control List following the recommendations of the user manual "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 network segmentation and configure a firewall to block all unauthorized access to TCP ports 502 and 80 • Disable the HTTP service and other communications services (FTP, SMTP, etc.) when not needed or restrict access to authorized users

	Please note these mitigations may not be sufficient on older product firmware versions. Products must be updated to the most current version available: • M340 CPU v3.40 : https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_xx.xx/ • Quantum 140CPU65xxx Copro v6.1 : https://www.se.com/fr/fr/download/document/140CPU65260+Quantum+Copro+Exec+and+Release+Notes/ • Premium TSXP57xxx Copro v6.1: TSXP574634M Ethernet Copro Firmware | Schneider Electric (se.com)
Modicon M340 ethernet modules: BMXNOC0401 BMXNOE01* BMXNOR0200H *All versions*	Customers should immediately apply the following mitigations to reduce the risk of exploit. For further details please check the Cyber Security Reference Manual available here: Modicon Controllers Platform - Cyber Security, Reference Manual User guide | Schneider Electric • Setup a VPN between the Modicon PLC modules and the engineering workstation containing EcoStruxure Control Expert or EcoStruxure Process Expert. For the **M340 offer**, the recommended configuration is described in the section "**How to protect M340 architectures with EAGLE40 using a VPN**" of the EcoStruxure Control Expert online help. • Configure the Access Control List following the recommendations of the user manual "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 network segmentation and configure a firewall to block all unauthorized access to TCP ports 502 and 80 • Disable the HTTP service and other communications services (FTP, SMTP, etc.) when not needed or restrict access to authorized users Please note these mitigations may not be sufficient on older product firmware versions. Products must be updated to the most current version available: • BMXNOE0110 v6.60 https://www.se.com/ww/en/download/document/BMXNOE0110%20Exec%20and%20Release%20Notes/?searchSource=guided • BMXNOE0100 v3.40 https://www.se.com/ww/en/download/document/BMXNOE0100%20Exec%20and%20Release%20Notes/?searchSource=guided

	• BMXNOC0401 v2.10 https://www.se.com/ww/en/download/document/BMXNOC0401%20Exec%20and%20Release%20Notes/?searchSource=guided • BMXNOR0200H v1.70 IR23: https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/?searchSource=guided
Modicon Quantum and Premium factory cast communication modules: 140NOE77111 140NOC78*00 TSXETY5103 and TSXETY4103 *All versions*	Customers should immediately apply the following mitigations to reduce the risk of exploit. For further details please check the Cyber Security Reference Manual available here: Modicon Controllers Platform - Cyber Security, Reference Manual User guide | Schneider Electric • Setup network segmentation and configure the firewall to block all unauthorized access to TCP ports 502 and 80 • Disable the HTTP service and other communications services (FTP, SMTP, etc) when not needed or restrict access to authorized users Please note these mitigations may not be sufficient on older product firmware versions. Products must be updated to the most current version available: • 140NOE771x1 v7.3: https://www.se.com/ww/en/download/document/140NOE77111+Exec+and+Release+Notes+For+Unity+and+Non+Unity+Users/ • 140NOC78*00 v1.74 : https://www.se.com/ww/en/download/document/140NOC78000+Exec+and+Release+Notes/ • TSXETY5103 v6.4: https://www.se.com/ww/en/download/document/TSXETY5103Exec/?searchSource=guided • TSXETY4100 v6.2: https://www.se.com/ww/en/download/document/TSXETY4103Exec and Release Notes/?searchSource=guided

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.

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

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 *11 January 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.01.07 14:01:41 -08'00'