Schneider Electric Security Notification

Modicon M340 Controller and Communication Modules

12 April 2022 (14 February 2023)

Overview

Schneider Electric is aware of a vulnerability in its Modicon M340 Controller and Communication Modules.

The Modicon M340 offers compactness, flexibility, scalability, and robustness for the process industry and a wide range of demanding automation applications.

Failure to apply the remediation and mitigations provided below may risk Denial of Service to the Ethernet communication, which could result in a loss of availability of the controller.

February 2023 Update: A remediation is available for Modicon M340 Ethernet Communication Modules BMXNOE0100 (H) and BMXNOE0110 (H) (page 2).

Affected Products and Versions

Product	Version
Modicon M340 CPUs	BMXP34* versions prior to V3.40
Modicon Ethernet Communication modules: BMXNOE0100 (H) BMXNOE0110 (H) BMXNOR0200H RTU	BMXNOE0100 (H) versions prior to SV03.50 BMXNOE0110 (H) versions prior to SV06.70 BMXNOR* versions prior to v1.7 IR24

Vulnerability Details

CVE ID: **CVE-2022-0222**

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-269: Improper Privilege Management* vulnerability exists that could cause a denial of service of the Ethernet communication of the controller when sending a specific request over SNMP.

Remediation & Mitigations

Affected Product & Version	Remediation & Mitigations
Modicon M340 *V3.40 and prior*	Version 3.50 of Modicon M340 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_03.50/ If customers choose not to apply the remediation provided above, they 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 161/UDP. • 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 a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert.
Modicon M340 Ethernet Communication Modules **BMXNOE0100 (H)** *Versions prior to SV03.50* **BMXNOE0110 (H)** *Versions prior to SV06.70*	Version SV03.50 of BMXNOE0100 (H) includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMXNOE0100_SV_03.50/ Version SV06.70 of BMXNOE0110 (H) includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMXNOE0110_SV_06.70/ If customers choose not to apply the remediation, then they 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 161/UDP. • 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/

Schneider Electric Security Notification

Modicon M340 X80 Ethernet Communication Module BMXNOR0200H RTU *Versions prior to V1.7 IR24*	Modicon M340 X80 Ethernet Communication Module BMXNOR0200H V1.7 IR24 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/BMXNOR0200H/ethernet-serial-rtu-module-2-x-rj45/ If customers choose not to apply the remediation provided above, they 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 161/UDP. • Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert.

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.

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 Security Notification

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2022-0222	Peter Cheng from ELEX FEIGONG RESEARCH INSTITUTE

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.

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

Schneider Electric Security Notification

Revision Control:

Version 1.0 *12 April 2022*	Original Release
Version 2.0 *13 September 2022*	A remediation is available for Modicon M340 X80 Ethernet Communication Module BMXNOR0200H RTU (page 3).
Version 3.0 *14 February 2023*	A remediation is available for Modicon M340 Ethernet Communication Modules BMXNOE0100 (H) and BMXNOE0110 (H) (page 2).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.02.13 13:13:34 -05'00'