Schneider Electric Security Notification

SNMP Service on Modicon M340 and Associated Communication Modules

8 December 2020 (13 September 2022)

Overview

Schneider Electric is aware of a vulnerability in the Modicon M340 offer and associated communication modules.

Modicon M340 Programable Automation Controllers are used in industrial processes and infrastructure control.

Failure to apply the remediations provided below may risk unexpected modification of network parameters, which could result in making targeted devices unreachable.

September 2022 update: A remediation is available for Modicon M340 X80 Ethernet Communication module BMXNOC0401 (page 2).

Affected Products and Versions

Product	Version
Modicon M340 CPUs	BMXP34* versions prior to V3.30
Modicon M340 X80 Communication Ethernet modules	BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H versions prior to V1.7 IR22 BMXNOC0401 versions prior to v2.11

Vulnerability Details

CVE ID: **CVE-2020-7536**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: *Improper Check for Unusual or Exceptional Conditions* vulnerability exists that could cause the device to be unreachable when doing an unattended modification of network parameters over SNMP.

Remediations

Firmware versions below include a fix for this vulnerability and are available for download:

Affected Product & Versions	Remediation
BMXNOE0100 (H) *versions prior to V3.4*	Firmware V3.4 is available for download below: https://www.se.com/ww/en/download/document/BMXNOE0100 Exec and Release Notes/
BMXNOE0110 (H) *versions prior to V6.6*	Firmware V6.6 is available for download below: https://www.se.com/ww/en/download/document/BMXNOE0110 Exec and Release Notes/
Modicon M340 CPU BMXP34* *versions prior to V3.30*	Firmware V3.30 is available for all the product references. Follow this link and find the right firmware file based on model used: https://www.se.com/ww/en/product-range/1468-modicon-m340/?parent-subcategory-id=3950
BMXNOR0200H *versions prior to V1.7 IR22*	Firmware V1.7 IR22 is available for download below: https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/
BMXNOC0401 *versions prior to V2.11*	Firmware V2.11 is available for download below: https://www.se.com/ww/en/product/BMXNOC0401/

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 following mitigations to reduce the risk of exploit:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 161/UDP 162/UDP.

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 Name
CVE-2020-7536	VAPT Team (C3i IITK, UP, India)

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, please contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

"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

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 *08 December 2020*	Original Release
Version 2.0 *09 February 2021*	BMXNOC0401 added as an affected product (page 1) Remediation section now includes BMXNOR0200H (page 2)
Version 3.0 *13 September 2022*	A remediation is available for Modicon M340 X80 Ethernet Communication module BMXNOC0401 (page 2).

Product Security Office

Digitally signed by Product Security Office
Date: 2022.09.09 15:54:28 -04'00'