Schneider Electric Security Notification

Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (V2.0)

8 December 2020 (10 August 2021)

Overview

Schneider Electric is aware of a vulnerability in the web server of the Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their associated communication modules.

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

Failure to apply the remediations provided below may risk execution of commands on the webserver by an unauthenticated attacker, which could result in loss of availability and integrity on the controller.

August 2021 Update: Added remediation for the Modicon X80 BMXNOR0200H RTU Module (page 4).

Affected Products and Versions

Product	Version
Modicon M340 CPUs	BMXP34* all versions prior to V3.30
Modicon M340 Ethernet Communication modules	BMXNOE0100 (H) all versions prior to V3.3 BMXNOE0110 (H) all versions prior to V6.5 BMXNOC0401 (H) all versions prior to V2.10
Modicon Premium communication modules	TSXETY4103 prior to V6.2 TSXETY5103 prior to V6.4
Modicon Premium processors with integrated Ethernet COPRO	TSXP574634 versions prior to V6.1 TSXP575634 versions prior to V6.1 TSXP576634 versions prior to V6.1
Modicon Quantum processors with integrated Ethernet COPRO	140CPU65xx0 prior to V6.1
Modicon Quantum communication modules	140NOE771x1, prior to V7.1 140NOC78x00, prior to V1.74 140NOC77101, prior to V1.08
Modicon X80 BMXNOR0200H RTU module	BMXNOR200H all versions prior to V1.70 IR 23

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-7540**

CVSS v3.0 Base Score 8.2 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists that could cause unauthenticated command execution in the controller when sending special HTTP requests.

Remediation

These vulnerabilities have been fixed or mitigated in the versions below.

Affected Product & Version	Remediation/Mitigation
Modicon M340 CPU BMXP34* prior to V3.30	Firmware V3.30 is available for all of 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 If customers choose not to apply the remediation, see Mitigation section below
Modicon M340 Ethernet Communication modules BMXNOE0100 (H) prior to V3.3	Firmware V3.3 is available for download below https://www.se.com/ww/en/download/document/BMXNOE0100 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon M340 Ethernet Communication modules BMXNOE0110 (H) prior to V6.5	Firmware V6.5 is available for download below https://www.se.com/ww/en/download/document/BMXNOE0110 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon M340 Ethernet Communication modules BMXNOC0401 (H) prior to V2.10	Firmware V2.10 is available for download below https://www.se.com/ww/en/download/document/BMXNOC0401 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below

Schneider Electric Security Notification

Modicon Premium communication modules TSXETY4103 prior to V6.2	Firmware V6.2 is available for download below https://www.se.com/ww/en/download/document/TSXETY4103 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Premium communication modules TSXETY5103 prior to V6.4	Firmware V6.4 is available for download below https://www.se.com/ww/en/download/document/TSXETY5103 Exec/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Premium processors with integrated Ethernet COPRO : TSXP574634 versions prior to V6.1 TSXP575634 versions prior to V6.1 TSXP576634 versions prior to V6.1	Firmware V6.1 is available for download below https://www.se.com/ww/en/download/document/TSXP574634M Premium Copro Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Quantum processors with integrated Ethernet COPRO 140CPU65xx0 prior to V6.1	Firmware V6.1 is available for download below https://www.se.com/ww/en/download/document/140CPU65260 Quantum Copro Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Quantum communication modules 140NOE771x1 prior to V7.1	Firmware V7.1 is available for download below https://www.se.com/ww/en/download/document/140NOE77101 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Quantum communication modules 140NOC 78x 00 prior to V1.74	Firmware V1.74 is available for download below https://www.se.com/ww/en/download/document/140NOC78100 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below
Modicon Quantum communication modules 140NOC77101 prior to V1.08	Firmware V1.08 is available for download below https://www.se.com/ww/en/download/document/140NOC77101 Exec and Release Notes/ If customers choose not to apply the remediation, see Mitigation section below

BMXNOR200H all versions prior to V1.70 IR 23	Firmware V1.70 IR 23 is available for download below https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/ If customers choose not to apply the remediation, see Mitigation section below

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.

Customers are advised that the web server is disabled by default. Because web services are only necessary for specific maintenance, configuration or monitoring activities, it is advised to disable web services all together during times when the services are not needed.

Mitigations

If customers choose not to apply the remediations provided in the remediation section, they should immediately apply the following mitigations to reduce the risk of exploit:

Modicon M340 CPU BMXP34* and Ethernet communication modules (BMXNOR0200H included)

- 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/
- Disable the Web server using 'Web Access (HTTP)' via UnityPro / EcoStruxure Control Expert using the following guideline: "Modicon M340 for Ethernet - Communication Modules and Processors, User Manual" in the chapter "Security / Security features": https://www.se.com/ww/en/download/document/31007131K01000.
  This is disabled by default when a new application is created

Modicon Premium and associated communication Modules:

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.

- 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/

- Disable the Web server using 'Web Access (HTTP)' via UnityPro / EcoStruxure Control Expert using the following guideline "Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual" in the chapter "Security Service Configuration Parameters / Security (Enable / Disable HTTP, FTP, and TFTP)".

  https://www.se.com/ww/en/download/document/35006192K01000

  This is disabled by default when a new application is created.

Modicon Quantum and associated communication modules:

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.

- 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/
- Disable the Web server using 'Web Access (HTTP)' via UnityPro / EcoStruxure Control Expert using the following guideline " Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual" in the chapter "Security (Enable / Disable HTTP, FTP, and TFTP)":
  https://www.se.com/ww/en/download/document/33002479K01000

  This is disabled by default when a new application is created.

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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2020-7540	• DongJian Security Lab @ DingXiang ICS • Peter Cheng from CyberSpace Non-Attack Research Institute of Elex Cybersecurity Inc.

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. 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

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 *8 December 2020*	Original Release
Version 2.0 *10 August 2021*	Added remediation for the Modicon X80 BMXNOR0200H RTU Module (page 4).

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:50:36 -04'00'