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 (11 May 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 associated communication modules.

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

Failure to apply the remediations provided below may risk an attack on the web server, which could result in disclosure of sensitive information.

May 2021 Update: Added all versions of BMXNOC0401 to the affected products table.

Affected Products and Versions

Product	Version
Modicon M340 CPUs	BMXP34* versions prior to V3.30
Modicon M340 Ethernet Communication modules	BMXNOE0100 (H) prior to version 3.4 BMXNOE0110 (H) prior to version 6.6 BMXNOC0401 all versions
Modicon Premium processors with integrated Ethernet COPRO	TSXP574634 all versions TSXP575634 all versions TSXP576634 all versions
Modicon Quantum processors with integrated Ethernet COPRO	140CPU65xxxxx all versions
Modicon Quantum communication modules	140NOE771x1 versions prior to V7.3 140NOC78x00 all versions 140NOC77101 all versions
Modicon Premium communication modules	TSXETY4103 all versions TSXETY5103 all versions

Vulnerability Details

CVE ID: **CVE-2020-7535**

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

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type)* vulnerability exists that could cause disclosure of information when sending a specially crafted request to the controller over HTTP.

Remediation

This vulnerability has been fixed or mitigated in the versions below.

Affected Product & Version	Remediation/Mitigation
Modicon M340 CPU BMXP34* prior to version 3.30	Firmware version 3.30 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 If customers choose not to apply the remediation, see Mitigation section below
Modicon M340 Ethernet Communication modules BMXNOE0100 (H) prior to version 3.4	Firmware version 3.4 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 version 6.6	Firmware version 6.6 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 TCP/IP network module BMXNOC0401 all versions	Schneider Electric is establishing a remediation plan for all future versions of this product. 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

Schneider Electric Security Notification

Modicon Quantum communication modules 140NOE771x1 prior to version 7.3	Firmware V7.3 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 processors with integrated Ethernet COPRO – 140CPU65xxxxx all versions	**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. To mitigate the risks, users should immediately: • 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
Modicon Quantum communication modules – 140NOC78x00 all versions 140NOC77101 all versions	
Modicon Premium processors with integrated Ethernet COPRO – TSXP574634 all versions TSXP575634 all versions TSXP576634 all versions	**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. To mitigate the risks, users should immediately: • 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 For further information, please check the "Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual" and the Modicon Controllers Platform Cyber Security Reference Manual
Modicon Premium communication modules – TSXETY4103 all versions TSXETY5103 all versions	

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 above and until remediation for BMXNOC0401 will be available, they should immediately apply the following mitigations to reduce the risk of exploit:

Modicon M340 CPU BMXP34* and Ethernet communication modules

To mitigate the risks, users should immediately:

- 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.

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.

To mitigate the risks, users should immediately:

- 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

Schneider Electric Security Notification

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.

Acknowledgements

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

CVE	Researcher
CVE-2020-7535	• Zheng Qiang • 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, 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

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.

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 *11 May 2021*	Added all versions of BMXNOC0401 to the affected products table. (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 21:32:34 -04'00'