# 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 multiple vulnerabilities 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 a disclosure of information and a Denial of Service attack, which could result in the unavailability of the controller.

August 2021 Update: Added remediation for the Modicon Ethernet Communication / Serial RTU BMXNOR0200H module (page 2).

## Affected Products and Versions

| Product | Version |
|---|---|
| Modicon M340 CPUs | BMXP34* versions prior to V3.30 |
| Modicon M340 Ethernet Communication modules | BMXNOE0100 (H) versions prior to V3.3<br>BMXNOE0110 (H) versions prior to V6.5<br>BMXNOC0401 (H) versions prior to V2.10<br>BMXNOR0200H RTU versions prior to V1.70 IR23 |
| Modicon Premium communication modules | TSXETY4103 versions prior to V6.2<br>TSXETY5103 versions prior to V6.4 |
| Modicon Premium processors with integrated Ethernet COPRO | TSXP574634 versions prior to V6.1<br>TSXP575634 versions prior to V6.1<br>TSXP576634 versions prior to V6.1 |
| Modicon Quantum processors with integrated Ethernet COPRO | 140CPU65xx0 versions prior to V6.1 |
| Modicon Quantum communication modules | 140NOE771x1 versions prior to V7.1<br>140NOC78x00 versions prior to V1.74<br>140NOC77101 versions prior to V1.08 |

## Vulnerability Details

CVE ID: **CVE-2020-7541**

CVSS v3.0 Base Score 5.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

A CWE-425: Direct Request ('Forced Browsing') vulnerability exists that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP.

CVE ID: **CVE-2020-7539**

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 a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP.

## Remediation

These vulnerabilities have been fixed in the versions listed below.

| Affected Product & Version | Remediation |
|---|---|
| Modicon M340 CPU<br>BMXP34*<br>Versions prior to V3.30 | Firmware version 3.30 is available for all the product references. Follow this link and find the right firmware file based on model used.<br>https://www.se.com/ww/en/product-range/1468-modicon-m340/?parent-subcategory-id=3950 |
| Modicon M340 Ethernet Communication modules<br>BMXNOE0100 (H)<br>Versions prior to V3.3 | Firmware version 3.3 is available for download below<br>https://www.se.com/ww/en/download/document/BMXNOE0100 Exec and Release Notes/ |
| Modicon M340 Ethernet Communication modules<br>BMXNOE0110 (H)<br>Versions prior to V6.5 | Firmware version 6.5 is available for download below<br>https://www.se.com/ww/en/download/document/BMXNOE0110 Exec and Release Notes/ |
| Modicon M340 Ethernet Communication modules<br>BMXNOC0401(H)<br>Versions prior to V2.10 | Firmware version 2.10 is available for download below<br>https://www.se.com/ww/en/download/document/BMXNOC0401 Exec and Release Notes/ |
| Modicon Ethernet Communication / Serial RTU module<br>BMXNOR0200H<br>Versions prior to V1.70 IR23 | Firmware version 1.70 IR23 is available for download below<br>https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/ |

| | |
|---|---|
| Modicon Premium processors with integrated Ethernet COPRO:<br>TSXP574634 versions prior to V6.1<br>TSXP575634 versions prior to V6.1<br>TSXP576634 versions prior to V6.1 | Firmware version 6.1 is available for download below<br>https://www.se.com/ww/en/download/document/TSXP574634M Premium Copro Exec and Release Notes/ |
| Modicon Premium communication modules TSXETY4103<br>Versions prior to V6.2 | Firmware version 6.2 is available for download below<br>https://www.se.com/ww/en/download/document/TSXETY4103 Exec and Release Notes/ |
| Modicon Premium communication modules TSXETY5103<br>Versions prior to V6.4 | Firmware version 6.4 is available for download below<br>https://www.se.com/ww/en/download/document/TSXETY5103 Exec/ |
| Modicon Quantum processors with integrated Ethernet COPRO version 6.1 product reference 140CPU65xx0<br>Versions prior to V6.1 | Firmware version 6.1 is available for download below<br>https://www.se.com/ww/en/download/document/140CPU65260 Quantum Copro Exec and Release Notes/ |
| Modicon Quantum communication modules 140NOE771x1<br>Versions prior to V7.1 | Firmware version 7.1 is available for download below<br>https://www.se.com/ww/en/download/document/140NOE77101 Exec and Release Notes/ |
| Modicon Quantum communication modules 140NOC78x00<br>Versions prior to V1.74 | Firmware version 1.74 is available for download below<br>https://www.se.com/ww/en/download/document/140NOC78100 Exec and Release Notes/ |
| Modicon Quantum communication modules 140NOC77101<br>Versions prior to V1.08 | Firmware version 1.08 is available for download below<br>https://www.se.com/ww/en/download/document/140NOC77101 Exec and Release Notes/ |

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:

- Set up network segmentation and implement a firewall to block all unauthorized access to HTTP port 80/TCP on the controllers.
- Disable HTTP service via EcoStruxure Control Expert. This is disabled by default when a new application is created.
- Configure the Access Control List following the recommendation on the "Modicon Controllers Platform Cyber Security Reference Manual"

## 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-2020-7539 | DongJian Security Lab @ DingXiang ICS |
| CVE-2020-7541 | BDU FSTEC Russia |

## 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

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**<br>*8 December 2020* | Original Release |
| **Version 2.0**<br>*10 August 2021* | A fix is available on the Modicon Ethernet Communication / Serial RTU BMXNOR0200H module (page 2). |

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:49:21 -04'00'