

## Schneider Electric Security Notification

### Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules

10 November 2020 (14 February 2023)

#### Overview

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

The [Modicon Ethernet Programmable Automation](#) products are controllers for industrial process and infrastructure.

Failure to apply the mitigations provided below may risk write access and the execution of commands, which could result in corruption of data, or crash of the web server.

**February 2023 Update:** A remediation is available on Modicon M340 Ethernet Communication Modules BMXNOE0100 (H) and BMXNOE0110 (H) ([page 3](#)).

#### Affected Products and Versions

Product	Versions
<b>M340 CPUs</b>	M340 P34x versions prior to V3.40
<b>Modicon Ethernet Communication Modules</b>	BMXNOE0100 (H) Versions prior to SV03.50 BMXNOE0110 (H) Versions prior to SV06.70 BMXNOC0401 Versions prior to V2.11 BMXNOR0200H Versions prior to V1.7 IR 23
<b>Premium Processors with Integrated Ethernet COPRO</b>	TSXP574634, TSXP575634, TSXP576634 All versions
<b>Premium Communication Modules</b>	140CPU65xxxxx, All versions
<b>Quantum Communication Modules</b>	140NOE771x1 All versions 140NOC78x00 All versions 140NOC77101 All versions

#### Vulnerability Details

CVE ID: **CVE-2020-7562**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H

A CWE-125: *Out-of-Bounds Read* vulnerability exists which could cause a segmentation fault or a buffer overflow when uploading a specially crafted file on the controller over FTP.

## Schneider Electric Security Notification

CVE ID: **CVE-2020-7563**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0 AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H

A CWE-787: *Out-of-bounds Write* vulnerability exists which could cause corruption of data, a crash, or code execution when uploading a specially crafted file on the controller over FTP.

CVE ID: **CVE-2020-7564**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0 AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H

A CWE-120: *Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')* vulnerability exists which could cause write access and the execution of commands when uploading a specially crafted file on the controller over FTP.

### Remediation

Affected Products	Remediation
<b>M340 CPUs</b> <b>BMXP34x</b> <i>Prior to V3.40</i>	V3.40 of M340 CPUs includes a fix for these vulnerabilities and is available for download here: <a href="https://www.se.com/ww/en/download/document/BMXP34xxxx_SV_xx.xx/">https://www.se.com/ww/en/download/document/BMXP34xxxx_SV_xx.xx/</a>
<b>Modicon Ethernet Communication Modules</b> <b>BMXNOR0200H</b> <i>Prior to V1.7 IR 23</i>	V1.70 IR23 of BMXNOR0200H includes a fix for these vulnerabilities and is available for download here: <a href="https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/">https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/</a>
<b>Modicon Ethernet Communication Modules</b> <b>BMXNOC0401</b> <i>Prior to V2.11</i>	V2.11 of BMXNOC0401 includes a fix for these vulnerabilities and is available for download here: <a href="https://www.se.com/ww/en/product/BMXNOC0401/ethernet-tcp-ip-network-module-modicon-m340-automation-platform-4-x-rj45-10-100/">https://www.se.com/ww/en/product/BMXNOC0401/ethernet-tcp-ip-network-module-modicon-m340-automation-platform-4-x-rj45-10-100/</a>

## Schneider Electric Security Notification

**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/](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/](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 80/HTTP (Note HTTP is disabled by default).
- 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 or Process Expert.

## Schneider Electric Security Notification

<p><b>Premium processors with integrated Ethernet COPRO</b> <b>TSXP574634, TSXP575634, TSXP576634, All versions</b></p> <p><b>Premium communication modules</b> <b>TSXETY4103 All versions</b> <b>TSXETY5103 All versions</b></p>	<p>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.</p> <p>Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.</p> <p>Customers should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> <li>• 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”: <a href="https://www.se.com/ww/en/download/document/35006192K01000/">https://www.se.com/ww/en/download/document/35006192K01000/</a></li> <li>• Setup network segmentation and implement a firewall to block all unauthorized access to port 21/TCP</li> </ul>
<p><b>Quantum processors with integrated Ethernet COPRO</b> <b>140CPU65xxxxx, All versions</b></p> <p><b>Quantum communication modules</b> <b>140NOE771x1 All versions</b> <b>140NOC78x00 All versions</b> <b>140NOC77101 All versions</b></p>	<p>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.</p> <p>Customers should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> <li>• 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”: <a href="https://www.se.com/ww/en/download/document/33002467K01000/">https://www.se.com/ww/en/download/document/33002467K01000/</a></li> <li>• Setup network segmentation and implement a firewall to block all unauthorized access to port 21/TCP</li> </ul>

## Schneider Electric Security Notification

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.

To ensure you are informed of all updates, including details on affected products and remediation plans, please subscribe to Schneider Electric's security notification service here:

<https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp>

### 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 these vulnerabilities:

CVE	Researcher
CVE-2020-7562 CVE-2020-7563 CVE-2020-7564	Kai Wang of Fortinet's FortiGuard Labs

# Schneider Electric Security Notification

## 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>

## 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

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](http://www.se.com)

## Schneider Electric Security Notification

Revision Control:

<b>Version 1.0</b> <i>10 November 2020</i>	Original Release
<b>Version 2.0</b> <i>10 August 2021</i>	Added remediation for M340 CPU and BMXNOR0200H.
<b>Version 3.0</b> <i>13 September 2022</i>	A remediation is available for Modicon M340 X80 Ethernet Communication Module BMXNOC0401 (page 2).
<b>Version 4.0</b> <i>14 February 2023</i>	A remediation is available on Modicon M340 Ethernet Communication Modules BMXNOE0100 (H) and BMXNOE0110 (H) ( <a href="#">page 3</a> ).