# Schneider Electric Security Notification

## Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules (V2.0)

**10 November 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 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.

August 2021 Update: Added remediation for M340 CPU and BMXNOR0200H (page 2).

## Affected Products and Versions

| Product | Versions |
|---|---|
| **M340 CPUs** | MX P34x versions prior to 3.40 |
| **M340 Communication Ethernet modules** | BMX NOE 0100 (H) all versions<br>BMX NOE 0110 (H) all versions<br>BMX NOC 0401 all versions<br>BMX NOR 0200H versions prior to 1.7 IR 23 |
| **Premium processors with integrated Ethernet COPRO** | TSXP574634, TSXP575634, TSXP576634, all version |
| **Premium communication modules** | 140CPU65xxxxx, all versions |
| **Quantum communication modules** | 140NOE771x1 all versions<br>140NOC78x00 all versions<br>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 |
|---|---|
| **M340 CPUs**<br>BMX P34x versions prior to 3.40 | A fix is available on version 3.40 available for download here:<br>https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_xx.xx/ |
| **M340 Communication Ethernet modules**<br>BMX NOR 0200H versions prior to 1.7 IR 23 | A fix is available on version 1.70 IR23 available for download here:<br>https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/ |
| **M340 Communication Ethernet modules**<br>BMX NOE 0100 (H) all versions<br>BMX NOE 0110 (H) all versions<br>BMX NOC 0401 all versions | Schneider Electric is establishing a remediation plan to ensure all current and future versions of Modicon PAC controllers will include a fix for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the mitigations listed below to reduce the risk of exploit |

| | |
|---|---|
| **Premium processors with integrated Ethernet COPRO**<br>TSXP574634, TSXP575634, TSXP576634, all version<br><br>**Premium communication modules**<br>TSXETY4103 all versions<br>TSXETY5103 all versions | 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.<br>Customers should immediately apply the following mitigations to reduce the risk of exploit:<br><br>• 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/<br>• Setup network segmentation and implement a firewall to block all unauthorized access to port 21/TCP |
| **Quantum processors with integrated Ethernet COPRO**<br>140CPU65xxxxx, all versions<br><br>**Quantum communication modules**<br>140NOE771x1 all versions<br>140NOC78x00 all versions<br>140NOC77101 all versions | 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.<br>Customers should immediately apply the following mitigations to reduce the risk of exploit:<br>• 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/<br>• Setup network segmentation and implement a firewall to block all unauthorized access to port 21/TCP |

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.

## Mitigations

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

- Disable FTP via UnityPro / Ecostruxure Control Expert. This is disabled by default when a new application is created.
- Configure the Access Control list via Ecostruxure Control Expert programming tool.
- Setup network segmentation and implement a firewall to block all unauthorized access to port 21/TCP.

For further information please refers to "Modicon Controllers Platform - Cyber Security, Reference Manual" https://www.se.com/ww/en/download/document/EIO0000001999/

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.

# Schneider Electric Security Notification

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


## 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

## 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>*10 November 2020* | Original Release |
| **Version 2.0**<br>*10 August 2021* | Added remediation for M340 CPU and BMXNOR0200H |

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:41:59 -04'00'