Schneider Electric Security Notification

Web Server on Modicon M340, Legacy Offers Modicon Quantum and Premium and Associated Communication Modules

14 September 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in the web server component of the Modicon M340 PLC offer. In addition, the Modicon Quantum and Modicon Premium Legacy offers and associated communication modules are affected.

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

Failure to apply the remediations provided below may risk an attack via the web server, which could result in disclosure of sensitive information or Denial of Service of the controller.

Affected Products and Versions

Product	Version
Modicon M340 CPUs	BMXP34* versions prior to V3.40
Modicon M340 X80 Ethernet Communication modules	BMXNOE0100 (H) all versions BMXNOE0110 (H) all versions BMXNOC0401 all versions BMXNOR0200H RTU 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 all versions 140NOC78x00 all versions 140NOC77101 all versions
Modicon Premium communication modules	TSXETY4103 all versions TSXETY5103 all versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2021-22785**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A *CWE-200: Information Exposure* vulnerability exists that could cause sensitive information of files located in the web root directory to leak when an attacker sends a HTTP request to the web server of the device.

CVE ID: **CVE-2021-22788**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-787: Out-of-bounds Write* vulnerability exists that could cause denial of service when an attacker sends a specially crafted HTTP request to the web server of the device.

CVE ID: **CVE-2021-22787**

CVSS v3.1 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-20: Improper Input Validation vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request to the web server of the device.

Remediation

Schneider Electric encourages all industrial companies to ensure they have implemented cybersecurity best practices across their operations and supply chains to reduce cyber risks. Where appropriate this includes locating industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission critical systems and devices from being accessed from outside networks; systematically applying security patches. In addition, specific recommended actions on the impacted products are listed below.

Affected Product & Version	Remediation/Mitigation
Modicon M340 CPU BMXP34* prior to V3.40	V3.40 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_xx.xx/ If customers choose not to apply the remediation, see the mitigation section below.

Modicon M340 X80 Ethernet Communication modules BMXNOR0200H RTU prior to V1.70 IR23	V1.70 IR23 includes a fix for **CVE-2021-22785** vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMXNOR0200H_FW/ Schneider Electric is establishing a remediation plan to address **CVE-2021-22787** and **CVE-2021-22788** 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: • 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
Modicon M340 Ethernet Communication modules BMXNOE0100 (H) all versions	Schneider Electric is establishing a remediation plan for all future versions of these products. 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: • 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.
Modicon M340 Ethernet Communication modules BMXNOE0110 (H) all versions	
Modicon M340 Ethernet TCP/IP network module BMXNOC0401 all versions	Schneider Electric is establishing a remediation plan for all future versions of these products. 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: • Setup network segmentation and implement a firewall to block all unauthorized access to port 80/HTTP • Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert or Process Expert.

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 140NOE771x1 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	

Mitigations

Schneider Electric is establishing a remediation plan for all future versions of Modicon M340 X80 Ethernet Communication modules that will include a fix for these vulnerabilities. We will update this document when the remediation is available.

Mitigations described in the table above must be applied until then.

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

https://www.se.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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2021-22785 CVE-2021-22788 CVE-2021-22787	Peter Cheng from ELEX FEIGONG RESEARCH INSTITUTE

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

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 *14 September 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.09.11 08:57:32 -04'00'