Schneider Electric Security Notification

Embedded FTP Servers for Modicon PAC Controllers

22 March 2018 (13 August 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities in the FTP servers of its Modicon PAC controllers.

Modicon PACs (Programmable Automation Controllers) control and monitor industrial operations in a sustainable, flexible, efficient, and protected way. Our PLCs and PACs supply edge technology, augmenting it with Ethernet connectivity, built-in cybersecurity, and processing power needed to handle Big Data analysis and protect against new vulnerabilities among connected industrial assets, across devices or into the cloud.

Failure to address these vulnerabilities could result in unauthorized access to your PLC and a denial of service or other malicious activity.

August 2024 Update: A remediation is available for the Modicon M580 CPU Safety (page 4).

Affected Products and Versions

Affected Products and Versions	CVE-			
	2018-7242	2018-7241	2018-7240	2011-4859
Modicon M340, v3.50		X	X	X
Modicon M340, v3.40 and prior	X	X	X	X
Modicon M580 (part numbers BMEP* & BMEH*, excluding M580 CPU Safety), Versions prior to SV4.10	X	X	X	
Modicon M580 CPU Safety (part numbers BMEP58*S & BMEH58*S), Versions prior to SV4.21	X	X	X	
Modicon RTU: BMXNOR0200H, versions prior to v1.7 IR24	X	X	X	X
Modicon Ethernet Communication Modules: BMXNOE01*, All versions	X	X	X	X
Modicon X80 Ethernet Communication Modules: BMXNOC0401, versions prior to v2.11	X	X	X	X
Legacy Modicon Premium and Quantum, All versions	X	X	X	X

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2018-7240**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause arbitrary code execution or malicious firmware installation when FTP upgrade feature is enabled. Special command dedicated to firmware upgrade can be called to execute DoS attack. Also, malicious crafted firmware can be transferred and loaded into PLC causing unauthorized code execution.

CVE ID: **CVE-2018-7241**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-798: Use of Hard-coded Credentials vulnerability exists in the firmware that could cause access by an unauthorized user to the controller when FTP protocol is enabled.

CVE ID: **CVE-2011-4859**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-798: Use of Hard-coded Credentials vulnerability exists in the Operating System that could cause access by an unauthorized user to the controller when FTP protocol is enabled.

CVE ID: **CVE-2018-7242**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists that could make the algorithm used to encrypt the password vulnerable and make it easier for remote attackers to obtain access when hash collision attacks are executed over Telnet or FTP.

Remediations & Mitigations

Products & Affected Versions	Remediations & Mitigations
Modicon M340 *Versions prior to v3.50*	Version 3.50 of Modicon M340 includes a fix for CVE-2018-7242 vulnerability and is available for download here: https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_03.50/ 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: • Setup network segmentation and implement a firewall to block all unauthorized access to FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module.
Modicon M580 (part numbers BMEP* & BMEH*, excluding M580 CPU Safety) *Versions prior to SV4.10*	Firmware SV4.10 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMEx58x0x0_SV04.10/ If customers choose not to apply the remediation, then they are encouraged to immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module. • Ensure the CPU is running with the memory protection activated by configuring the input bit to a physical input, for more details refer to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual", "CPU Memory Protection section": https://www.schneider-electric.com/en/download/document/EIO0000001999/

	▪ NOTE: The CPU memory protection cannot be configured with Hot Standby CPUs. In such cases, use IPsec encrypted communication
Modicon M580 CPU Safety (part numbers BMEP58*S & BMEH58*S) *Versions prior to SV4.21*	Firmware SV4.21 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/62098-modicon-m580-pac-controller/#software-and-firmware Important: customer needs to use version of EcoStruxure™ Control Expert V16.0 HF001 minimum to connect with the latest version of M580 CPU Safety. The software is available for download here: https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware 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 FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module. To further reduce the attack surface on Modicon M580 CPU Safety: • Ensure the CPU is running in Safety mode and maintenance input is configured to maintain this Safety mode during operation – refer to the document Modicon M580 - Safety System Planning Guide - in the chapter “Operating Mode Transitions”: https://www.se.com/ww/en/download/document/QGH60283/
Modicon RTU BMXNOR0200H *Versions prior to v1.7 IR24*	Version 1.7 IR24 of BMXNOR0200H X80 RTU includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/BMXNOR0200H/ 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 FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module.

Modicon X80 Ethernet Communication Module BMXNOC0401 *Versions prior to v2.11*	Version 2.11 of Modicon X80 Ethernet Communication modules BMXNOC0401 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/BMXNOC0401/ 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 FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module.
Modicon X80 Ethernet Communication Module BMXNOE01 *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon X80 Ethernet Communication modules BMXNOE0100 (H). 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 FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module.
Legacy Modicon Premium and Quantum *All versions*	Schneider Electric's Modicon Premium and 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 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 associated to the FTP weaknesses, users should immediately: • Setup network segmentation and implement a firewall to block all unauthorized access to FTP port 21/TCP on the controllers. • Deactivate the FTP service when not needed. • Use Access Control List to restrict communication to the authorized IP addresses. Refer to the Configuring Access Control section in the user manual for each module.

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 these vulnerabilities:

CVE	Researchers
CVE-2018-7240	Meng Leizi, Zhang Daoquan, Kirill Chernyshov (Positive Technologies), Alexey Stennikov (Positive Technologies), Peter Cheng from ELEX FEIGONG RESEARCH INSTITUTE
CVE-2018-7241	Ilya Karpov (Positive Technologies), Kirill Chernyshov (Positive Technologies), Ivan Kurnakov (Positive Technologies), Nikita Maximov (Positive Technologies)
CVE-2018-7242	Ilya Karpov (Positive Technologies), Kirill Chernyshov (Positive Technologies)

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

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

Revision Control:

Version 1.0.0 *22 March 2018*	Original Release
Version 2.0.0 *11 May 2021*	Updated CVSS scores and addition of Modicon M580 and clarification on Modicon M340 affected products.

Version 3.0.0 *09 August 2022*	A fix is available for Modicon M340 v3.50 that addresses the CVE-2018-7242 vulnerability. The list of impacted offers and version details have been updated for CVE-2018-7240, CVE-2018-7241, CVE-2018-7242 and CVE-2011-4859 vulnerabilities.
Version 3.1.0 *06 September 2022*	The version number for Modicon M580that addresses these vulnerabilities has been updated from v4.01 to v4.02.
Version 4.0.0 *13 September 2022*	A remediation is available for Modicon X80 Ethernet Communication module BMXNOC0401 and BMXNOR0200H RTU.
Version 5.0.0 *11 October 2022*	Adding a clarification to the list of affected products by splitting Modicon M580 and Modicon M580 Safety CPU ranges. The purpose of the notification update is to inform customers that the latest fix Modicon M580 sv4.02 does not apply to the Safety range of M580. It is highly recommended that customers using Modicon M580 Safety ranges continue to implement the mitigations shared in this document.
Version 6.0.0 *13 December 2022*	The Modicon M580 sv4.02 firmware has been retracted for quality issues and is no longer available for download. Additional mitigations have been introduced for Modicon M580 CPU and M580 CPU Safety, and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.
Version 7.0.0 *14 February 2023*	A remediation is available for CVE-2018-7242 on Modicon M340 Ethernet Communication Modules BMXNOE0100 (H) and BMXNOE0110 (H).
Version 8.0.0 *14 March 2023*	Remediation for the Modicon M580 CPU is available for download.
Version 9.0.0 *13 August 2024*	A remediation is available for the Modicon M580 CPU Safety (page 4).

CPCERT

Digitally signed by CPCERT
Date: 2024.08.12 12:57:20 -04'00'