Schneider Electric Security Notification

Embedded FTP Servers for Modicon PAC Controllers (V2.0)

22 March 2018 (11 May 2021)

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.

May 2021 Update: Updated CVSS scores and addition of Modicon M580 and clarification on Modicon M340 affected products.

Affected Products and Versions

Modicon PAC controllers using FTP server including all versions of M580, M340, Legacy Premium and Quantum and all associated communication/expansion modules.

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

A *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.

Impacted versions:

- M580 offer – all versions. Schneider Electric is establishing a remediation plan for the future versions of M580 CPU controllers that will include a fix for the CVE-2018-7240. This document will be updated when the remediation is available.
- M340 offer – all versions
- Legacy Premium and Quantum offer – all versions
- Modicon communication/expansion modules – all versions

Schneider Electric Security Notification

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

A *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.

Impacted versions:

- M580 offer – all versions. Schneider Electric is establishing a remediation plan for the future versions of M580 CPU controllers that will include a partial fix for the CVE-2018-7241. However, for compatibility with existing communication modules, this vulnerability may still exist in legacy architecture. This document will be updated when the remediation is available.
- M340 offer – all versions
- Legacy Premium and Quantum offer – all versions
- Modicon communication/expansion modules – all versions

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

A 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.

Impacted versions:

- M340 offer – all versions. Schneider Electric is establishing a remediation plan for future versions of M340 CPU controllers that will include a fix for the CVE-2011-4859. This document will be updated when the remediation is available.
- Legacy Premium and Quantum offer – all versions

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

A *CWE-327: Use of a Broken or Risky Cryptographic Algorithm* 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.

Impacted versions:

- M340 offer – all versions. Schneider Electric is establishing a remediation plan for all future versions of M580 CPU controllers that will include a fix for the CVE-2018-7242. This document will be updated when the remediation is available.
- Legacy Premium and Quantum offer – all versions

Mitigations

FTP service is disabled by default. Because FTP services are only necessary for specific maintenance and configuration activities, we advise customers disable FTP services altogether during times when it is not needed.

FTP protocol is inherently unsecure and therefore should be used with care to avoid sensitive information disclosure and unauthorized access to the controllers.

Modicon M580

The following workarounds and mitigations can be applied by customers to reduce the risk:

- 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 using Unity Pro / EcoStruxure Control Expert software
- 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.
- Setup a secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual”, in chapter “Setup secured communications”: https://www.schneider-electric.com/en/download/document/EIO0000001999/
- To remove the confidentiality issue from FTP protocol, use a BMENOC module and follow the instructions to configure IPSEC feature as described in the guideline “Modicon M580 - BMENOC03.1 Ethernet Communications Module, Installation and Configuration Guide” in the chapter “Configuring IPSEC communications”: https://www.schneider-electric.com/en/download/document/HRB62665/

Modicon M340:

To mitigate the risks associated to the FTP weaknesses, users should immediately apply the following instructions.

- 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 Premium and Quantum:

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.

Schneider Electric Security Notification

Customers should strongly consider migrating to the ModiconM580 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.

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(s) for identifying and helping to coordinate a response to this vulnerability:

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)

Schneider Electric Security Notification

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

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

Schneider Electric Security Notification

Revision Control:

Version 1.0 *22 March 2018*	Original Release
Version 2.0 *11 May 2021*	Updated CVSS scores and addition of Modicon M580 and clarification on Modicon M340 affected products.

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 22:15:13 -04'00'