Security Notification - Embedded FTP Servers for Modicon

22-Mar-2018 **(Updated 6-Apr-2018)**

Overview

Schneider Electric has become aware of multiple vulnerabilities in the FTP servers of its Modicon PLC family of products. Please take the necessary steps now to secure your Modicon PLC. Failure to address these vulnerabilities could result in unauthorized access to your PLC and a denial of service or other malicious activity.

Vulnerability Overview

The reported vulnerabilities could enable unauthorized access to the file transfer service provided by the Modicon PLCs, which could result in arbitrary code execution or malicious firmware installation.

Product(s) Affected

The product(s) affected include all Modicon Premium, Quantum, M340 and BMXNOR0200 controllers.

Mitigations Details

Schneider Electric recommends customers follow the instructions outlined in the Modicon Controllers Platform Cyber Security Reference Manual to install your Modicon PLCs securely. We also recommend:

- Protecting access to the Modicon PLC via a firewall that restricts FTP access to the Modicon PLC network.
- FTP service is disabled by default. Because FTP services are only necessary for specific maintenance and configuration activities, we advise to disable FTP services altogether during times when the service is not needed.

For customers requiring additional support, Schneider Electric's Industrial Cybersecurity Services team are available to help with assessments and deployment support. Please visit us for more information: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Vulnerability Details

CVE	Vulnerability	Detailed description	CVSS Base score	Impacted products
CVE-2018-7240	Arbitrary code execution or malicious firmware installation	An FTP command used to upgrade the firmware of the module can be misused to cause a Denial of service, or in extreme cases, to load a malicious firmware	4.8 CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	All versions of Modicon Quantum communication modules
CVE-2018-7241	Hardcoded accounts	The FTP servers contain a hardcoded account	5.9 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H	All versions of communication modules for Modicon Premium, Quantum, M340 and BMXNOR0200
CVE-2018-7242	Vulnerable hash algorithms	The algorithm used to encrypt the password is vulnerable to hash collision attacks	5.9 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H	All versions of communication modules for Modicon Premium, Quantum, M340 and BMXNOR0200

Acknowledgements

Schneider Electric would like to the thank the following for helping to identify these vulnerabilities:

CVE-2018-7240

- Meng Leizi
- Zhang Daoquan
- Kirill Chernyshov (Positive Technologies)
- Alexey Stennikov (Positive Technologies)

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)

- Ivan Kurnakov (Positive Technologies)
- Nikita Maximov (Positive Technologies)

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *22 March 2018*	Original Release
Version 1.1 *30 March 2018*	Acknowledgements added
Version 1.2 *5 April 2018*	Acknowledgements updated

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.04.06 13:42:25 -04'00'