Schneider Electric Security Notification

Modicon Controllers

8 October 2019

Overview

Schneider Electric is aware of multiple vulnerabilities in three of its Modicon brand of programmable logic controllers.

Affected Product(s)

- Modicon M580 (all firmware versions)
- Modicon M340 (all firmware versions)
- Modicon BMxCRA and 140CRA modules (all firmware versions)

Vulnerability Details

CVE ID: **CVE-2019-6841**

CVSS v3.0 Base Score 4.9 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the PLC when upgrading the firmware with no firmware image inside the package using FTP protocol.

CVE ID: **CVE-2019-6842**

CVSS v3.0 Base Score 4.9 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the PLC when upgrading the firmware with a missing web server image inside the package using FTP protocol.

CVE ID: **CVE-2019-6843**

CVSS v3.0 Base Score 4.9 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the PLC when upgrading the controller with an empty firmware package using FTP protocol.

CVE ID: **CVE-2019-6844**

CVSS v3.0 Base Score 4.9 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service atack on the PLC when upgrading the controller with a firmware package containing an invalid web server image using FTP protocol.

CVE ID: **CVE-2019-6846**

CVSS v3.0 Base Score 6.5 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists, which could cause information disclosure when using the FTP protocol.

CVE ID: **CVE-2019-6847**

CVSS v3.0 Base Score 4.9 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-248: Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the FTP service when upgrading the firmware with a version incompatible with the application in the controller using FTP protocol.

Remediation

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:

To mitigate the risks associated to the FTP weaknesses, users should immediately:

- Set up 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 / Control Expert programming software.
- Change the default FTP password (this procedure should also be applied after each firmware upgrade of the controller) using Unity / Control Expert in the following menu: “Project Properties / Protection”
- When upgrading a firmware in the controller, make sure that the firmware downloaded is compatible with the application already available in the controller. If not the case, use Unity Pro / Control Expert software to rebuild your controller application.
- Set up 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:

- Set up 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.
- Change the default FTP password (this procedure should also be applied after each firmware upgrade of the controller) using Unity / Control Expert software in the following menu:
  "Project Properties / Protection"
- When upgrading a firmware in the controller, make sure that the firmware downloaded is compatible with the application already available in the controller. If not the case, use Unity Pro / Control Expert software to rebuild the application of your controller.

Modicon BMxCRA and 140CRA modules:

To mitigate the risks associated to the FTP weaknesses, users should immediately:

- Set up network segmentation and implement a firewall to block all unauthorized access to FTP port 21/TCP on the controllers.

Product Information

Ethernet Programmable Automation Controller for industrial process and infrastructure.

Product Category - All Categories

Learn more about Schneider Electric's product categories here:

www.schneider-electric.us/en/all-products

How to determine if you are affected

Affected products listed in this security notification connected to an Ethernet network

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6841, CVE-2019-6842, CVE-2019-6843, CVE-2019-6844, CVE-2019-6846	Jared Rittle (Cisco Talos)
CVE-2019-6847	Jared Rittle and Patrick DeSantis (Cisco Talos)

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 and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

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

Schneider Electric Security Notification

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *8-Oct-19*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.10.06 10:51:37 -04'00'