Schneider Electric Security Notification

Modicon Controllers

8 October 2019 (14 March 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities in the Modicon Controller products.

March 2023 Update: Remediation for the Modicon M580 CPU is available for download (page 3).

Affected Products & Remediations

Affected Products and Versions	CVE-					
	2019-6841	2019-6842	2019-6843	2019-6844	2019-6846	2019-6847
Modicon M580 (part numbers BMEP* & BMEH*, excluding M580 CPU Safety), Version prior to SV4.10	x	x	x	x	x	x
Modicon M580 CPU Safety (part numbers BMEP58*S & BMEH58*S), all versions	x	x	x	x	x	x
Modicon M340, all versions	x	x	x	x	x	x
Modicon BMxCRA and 140CRA modules, all versions	x	x	x	x	x	x

Vulnerability Details

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

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

A *CWE-755: Improper Handling of Exceptional Conditions* vulnerability exists which could cause a Denial of Service of the controller 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) | AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A *CWE-755: Improper Handling of Exceptional Conditions* vulnerability exists which could cause a Denial of Service of the controller when upgrading the firmware with a missing web server image inside the package using FTP protocol.

Schneider Electric Security Notification

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

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

A CWE-755: Improper Handling of Exceptional Conditions vulnerability exists which could cause a Denial of Service of the controller 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) | AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-755: Improper Handling of Exceptional Conditions vulnerability exists which could cause a Denial of Service of the controller 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 5.9 | (Medium) | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

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

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

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

A CWE-755: Improper Handling of Exceptional Conditions vulnerability exists which could cause a Denial of Service of the FTP service when upgrading the firmware with a version incompatible with the application in the controller using the FTP protocol.

Schneider Electric Security Notification

Remediation/Mitigations

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

Products & Affected Versions	Remediations & Mitigations
Modicon M580 CPU (part numbers BMEP* & BMEH*, excluding M580 CPU Safety) *SV4.10 and prior*	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 using Unity Pro / Control Expert 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 the application of your controller. • 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/ • Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter "Configuring the BMENUA0100 Cybersecurity Settings": https://www.se.com/ww/en/download/document/PHA83350 • 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/ • 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 and BMEH58*S) *All versions*	Schneider Electric is establishing a remediation plan for all future versions of M580 CPU Safety that will include a fix for this vulnerability. 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 using Unity Pro / Control Expert 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 the application of your controller. • 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/ • Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter “Configuring the BMENUA0100 Cybersecurity Settings”: https://www.se.com/ww/en/download/document/PHA83350 • 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/ 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 M340 *All versions*	Version 3.50 of Modicon M340 includes a fix for the 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. • 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 the application of your controller.
Modicon BMxCRA and 140CRA modules *All versions*	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.

Schneider Electric Security Notification

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.

Acknowledgement

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2019-6843, CVE-2019-6844, CVE-2019-6846, CVE-2019-6841, CVE-2019-6842	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

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

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 *26 Sep 2019*	Original Release

Schneider Electric Security Notification

Version 2.0 *10 Dec 2019*	Fix now available for M580 firmware version 3.10 for CVE-2019-6841, CVE-2019-6843, CVE-2019-6844 (pages 1-2,4-5)
Version 2.1 *15 April 2021*	Updated CWE for: • CVE-2019-6841 • CVE-2019-6842 • CVE-2019-6843 • CVE-2019-6844 • CVE-2019-6847
Version 3.0 *09 August 2022*	A fix is available in Modicon M580 V4.01 that addresses vulnerabilities related to FTP. The FTP protocol was previously required during the firmware upgrade process, it has now been replaced by the HTTPS protocol.
Version 3.1 *06 September 2022*	The version number for Modicon M580 that addresses these vulnerabilities has been updated from SV4.01 to SV4.02.
Version 4.0 *11 October 2022*	A clarification was added 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 (page 3).
Version 5.0 *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 (page 3) and M580 CPU Safety (page 4), and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.
Version 6.0 *14 March 2023*	Remediation for the Modicon M580 CPU is available for download (page 3).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.03.13 15:02:51 -04'00'