

Schneider Electric Security Notification

Modicon Controllers (V1.1)

10 December 2019 (24 March 2020)

Overview

Schneider Electric is aware of a vulnerability in the Modicon Controllers offers.

Affected Product(s)

- Modicon M580
- Modicon M340
- Modicon Quantum
- Modicon Premium

Vulnerability Details

CVE ID: **CVE-2019-6857**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a Denial of Service of the controller when reading specific memory blocks using Modbus TCP.

Impacted versions:

- **Modicon M580 all versions prior to V2.80** - A fix is available for this vulnerability on Modicon M580 firmware V3.10 firmware, links to fixed version in the [Download links section](#)
- **Modicon M340 all versions prior to V3.01** - A fix is available for this vulnerability on Modicon M340 V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Premium all versions prior to V3.20** - A fix is available for this vulnerability on Modicon Premium V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Quantum all versions prior to V3.60** - A fix is available for this vulnerability on Modicon Quantum V3.60 firmware, links to fixed version in the [Download links section](#)

Schneider Electric Security Notification

CVE ID: **CVE-2019-6856**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a Denial of Service when writing specific physical memory blocks using Modbus TCP.

Impacted versions:

- **Modicon M580 all versions prior to V2.80** - A fix is available for this vulnerability on Modicon M580 firmware V3.10 firmware, links to fixed version in the [Download links section](#)
- **Modicon M340 all versions prior to V3.01** - A fix is available for this vulnerability on Modicon M340 V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Premium all versions prior to V3.20** - A fix is available for this vulnerability on Modicon Premium V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Quantum all versions prior to V3.52** - A fix is available for this vulnerability on Modicon Quantum V3.60 firmware, links to fixed version in the [Download links section](#)

CVE ID: **CVE-2018-7794**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a Denial of Service when reading data with invalid index using Modbus TCP

Impacted versions:

- **Modicon M580 all versions prior to V2.80** - A fix is available for this vulnerability on Modicon M580 firmware V3.10 firmware, links to fixed version in the [Download links section](#)
- **Modicon M340 all versions prior to V3.01** - A fix is available for this vulnerability on Modicon M340 V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Premium all versions prior to V3.20** - A fix is available for this vulnerability on Modicon Premium V3.20 firmware, links to fixed version in the [Download links section](#)
- **Modicon Quantum all versions prior to V3.52** - A fix is available for this vulnerability on Modicon Quantum V3.60 firmware, links to fixed version in the [Download links section](#)

Schneider Electric Security Notification

Download Links

M580 V3.10 Firmware	
BMEP584040	https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV3.10/
BMEH584040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH584040_SV3.10/
BMEP586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV3.10/
BMEH586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV3.10/
BMEP581020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV3.10/
BMEP582020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV3.10/
BMEP582040 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV3.10/
BMEP583020	https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV3.10/
BMEP583040	https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV3.10/
BMEP584020	https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV3.10/
BMEP585040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV3.10/
BMEH582040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH582040_SV3.10/
BMEP584040S	https://www.schneider-electric.com/en/download/document/M580_BMEP584040S_SV3.10/
BMEH584040S	https://www.schneider-electric.com/en/download/document/M580_BMEH584040S_SV3.10/
BMEH586040S	https://www.schneider-electric.com/en/download/document/M580_BMEH586040S_SV3.10/
BMEP582040S	https://www.schneider-electric.com/en/download/document/M580_BMEP582040S_SV3.10/

Schneider Electric Security Notification

M340 V3.20 firmware	
BMXP3420302 and CL and H	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/
BMXP342020 and H	https://www.schneider-electric.com/en/download/document/BMXP342020_Firmwares/
BMXP342000	https://www.schneider-electric.com/en/download/document/BMXP342000_Firmwares/
BMXP341000 and H	https://www.schneider-electric.com/en/download/document/BMXP341000_Firmwares/
BMXP3420102 and CL	https://www.schneider-electric.com/en/download/document/BMXP3420102_Firmwares/
BMXP3420302	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/

Premium V3.20 firmware	
TSXP57104M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57104M_SV3.20
TSXP57154M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57154M_SV3.20
TSXP571634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP571634M_SV3.20
TSXP57204M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57204M_SV3.20
TSXP572634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP572634M_SV3.20
TSXP57254M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57254M_SV3.20
TSXP57304M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57304M_SV3.20
TSXP573634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP573634M_SV3.20
TSXP57354M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57354M_SV3.20
TSXP574634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP574634M_SV3.20
TSXP57454M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57454M_SV3.20

Schneider Electric Security Notification

TSXP575634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP575634M_SV3.20
TSXP57554M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP57554M_SV3.20
TSXP576634M [C]	https://www.schneider-electric.com/en/download/document/Premium_TSXP576634M_SV3.20
TSXH5724M [C]	Please contact your Schneider Electric customer support to get the firmware version 3.20
TSXH5744M [C]	Please contact your Schneider Electric customer support to get the firmware version 3.20

Quantum V3.60 firmware	
140CPU65150 [C] 140CPU65160 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU651X0_SV3.60
140CPU65260 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU65260_SV3.60
140CPU67261 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60
140CPU67060 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67060_SV3.60
140CPU67160 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67160_SV3.60
140CPU67261 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60
140CPU67260 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67260_SV3.60
140CPU65860 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU65860_SV3.60
140CPU67861 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU67861_SV3.60
140CPU65150 [C]	https://www.schneider-electric.com/en/download/document/Quantum_140CPU65150_SV3.60
140CPU65160S	Please contact your Schneider Electric customer support to get the firmware version 3.60
140CPU67160S	Please contact your Schneider Electric customer support to get the firmware version 3.60

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.

Acknowledgements

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

Schneider Electric Security Notification

CVE	Researcher(s) Name
CVE-2019-6857	Mengmeng Young, Gideon Guo
CVE-2019-6856	Chansim Deng
CVE-2018-7794	Younes Dragoni (Nozomi Networks)

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>

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

Schneider Electric Security Notification

Revision Control:

Version 1.0 <i>10 December 2019</i>	Original Release
Version 1.1 <i>24 March 2020</i>	Updated CVSS score for CVE-2018-7794 (page 2)