# Schneider Electric Security Notification

## Security Notification – Modicon Controllers (V2)

**14 May 2019 (13 August 2019)**

## Overview

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

## Affected Product(s)

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

## Vulnerabilities Details

CVE ID: **CVE-2018-7846**

CVSS v3.0 Base Score: 5.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

A CWE-501: Trust Boundary Violation vulnerability on connection to the Controller exists which could cause unauthorized access by conducting a brute force attack on Modbus protocol to the controller.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7849**

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-248: Uncaught Exception vulnerability exists which could cause a possible Denial of Service due to improper data integrity check when sending files the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7843**

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-248: Uncaught Exception vulnerability exists which could cause denial of service when reading memory blocks with an invalid data size or with an invalid data offset in the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.80** – A fix is available for this vulnerability on Modicon M580 firmware since V2.80, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

# Schneider Electric Security Notification

CVE ID: **CVE-2018-7848**

CVSS v3.0 Base Score: 5.9 | (Medium) | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-200: Information Exposure vulnerability exists which could cause the disclosure of SNMP information when reading files from the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7842**

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

A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of privilege by conducting a brute force attack on Modbus parameters sent to the controller.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7847**

CVSS v3.0 Base Score: 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-284: Improper Access Control vulnerability exists which could cause denial of service or potential code execution by overwriting configuration settings of the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7850**

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

A CWE-807: Reliance on Untrusted Inputs in a Security Decision vulnerability exists which could cause invalid information displayed in Unity Pro software.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7845**

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

A CWE-125: Out-of-bounds Read vulnerability exists which could cause the disclosure of unexpected data from the controller when reading specific memory blocks in the controller over Modbus.

Impacted versions:

- **Modicon M580 all versions prior to V2.80** – A fix is available for this vulnerability on Modicon M580 firmware V2.80, links to fixed version in the Download links section
- **Modicon M340 all versions** – A fix is available for this vulnerability on Modicon M340 firmware V3.01, links to fixed version in the Download links section

- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

CVE ID: **CVE-2018-7852**

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-248: Uncaught Exception vulnerability exists which could cause denial of service when an invalid private command parameter is sent to the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.80** – A fix is available for this vulnerability on Modicon M580 firmware V2.80, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.01** – A fix is available for this vulnerability on Modicon M340 firmware V3.01, links to fixed version in the Download links section
- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

CVE ID: **CVE-2018-7853**

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-248: Uncaught Exception vulnerability exists which could cause denial of service when reading invalid physical memory blocks in the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section

CVE ID: **CVE-2018-7854**

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-248 Uncaught Exception vulnerability exists which could cause a denial of Service when sending invalid debug parameters to the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this

vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section

- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section

CVE ID: **CVE-2018-7855**

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-248 Uncaught Exception vulnerability exists which could cause a Denial of Service when sending invalid breakpoint parameters to the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7856**

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-248: Uncaught Exception vulnerability exists which could cause a possible denial of Service when writing invalid memory blocks to the controller over Modbus.

Impacted versions:

- **Modicon M580 all versions prior to V2.80** – A fix is available for this vulnerability on Modicon M580 firmware V2.80, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2018-7857**

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-248: Uncaught Exception vulnerability exists which could cause a possible Denial of Service when writing out of bounds variables to the controller over Modbus.

Impacted versions:

- **Modicon M580 all versions** – A partial fix is available for this vulnerability on Modicon M580 firmware V2.80, links to fixed version in the Download links section, see additional recommendations in the Mitigations section
- **Modicon M340 all versions** – A partial fix is available for this vulnerability on Modicon M340 firmware V3.01, links to fixed version in the Download links section, see additional recommendations in the Mitigations section
- **Modicon Premium all versions** – A partial fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A partial fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

CVE ID: **CVE-2019-6806**

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

A CWE-200: Information Exposure vulnerability exists which could cause the disclosure of SNMP information when reading variables in the controller using Modbus

Impacted versions:

- **Modicon M580 all firmware versions** – See recommendations in the Mitigations section
- **Modicon M340 all firmware versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon M340 with a new NOC module, see recommendations in the Mitigations section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2019-6807**

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

A CWE-248: Uncaught Exception vulnerability exists which could cause a possible denial of service when writing sensitive application variables to the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

CVE ID: **CVE-2019-6808**

CVSS v3.0 Base Score: 10.0 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A CWE-284: Improper Access Control vulnerability exists which could cause a remote code execution by overwriting configuration settings of the controller over Modbus.

Impacted versions:

- **Modicon M580 firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90 (see Download links section) with Control Expert Hot Fix V14.0 (see Download links section)
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10 (see Download links section) with Control Expert Hot Fix V14.0 (see Download links section)
- **Modicon Premium all versions** –see recommendations in the Mitigations section
- **Modicon Quantum all versions** –see recommendations in the Mitigations section

CVE ID: **CVE-2018-7844**

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

A CWE-200: Information Exposure vulnerability exists which could cause the disclosure of SNMP information when reading memory blocks from the controller over Modbus.

Impacted versions:

- **Modicon M580 all versions** – See recommendations in the Mitigations section
- **Modicon M340 all versions** – See recommendations in the Mitigations section
- **Modicon Premium all versions** – See recommendations in the Mitigations section
- **Modicon Quantum all versions** – See recommendations in the Mitigations section

CVE ID: **CVE-2019-6830**

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-248: Uncaught Exception vulnerability exists which could cause a possible denial of service when sending an appropriately timed HTTP request to the controller.

Impacted versions:

- **Modicon M580 all versions prior to V2.80** – A fix is available for this vulnerability on Modicon M580 firmware V2.80, links to fixed version in the Download links section

CVE ID: **CVE-2019-6828**

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-248: Uncaught Exception vulnerability exists which could cause a possible denial of service when reading specific coils and registers in the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

CVE ID: **CVE-2019-6829**

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-248: Uncaught Exception vulnerability exists which could cause a possible denial of service when writing to specific memory addresses in the controller over Modbus.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section

CVE ID: **CVE-2019-6809**

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-248: Uncaught Exception vulnerability exists which could cause a possible denial of service when reading invalid data from the controller.

Impacted versions:

- **Modicon M580 with firmware version prior to V2.90** – A fix is available for this vulnerability on Modicon M580 firmware V2.90, links to fixed version in the Download links section
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.10, links to fixed version in the Download links section
- **Modicon Premium all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Premium V3.20, see recommendations in the Mitigations section
- **Modicon Quantum all versions** – A fix is scheduled for this vulnerability in Q1 2020 on Modicon Quantum V3.60, see recommendations in the Mitigations section

## Mitigations

The vulnerabilities described in this document are linked to weaknesses in the management of Modbus protocol. Customers using products with no fix available are strongly recommended to implement the mitigations listed below to reduce risk.

**Modicon M580:**

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

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Setup a secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual”, in chapter “Setup secured communications”: https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000001999.06.pdf&p_Doc_Ref=EIO0000001999
- 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/#page=1&toolbar=1&scrollbar=1&statusbar=1&view=fit

**Modicon M340:**

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

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List following the recommendations of the user manual "Modicon M340 for Ethernet Communications Modules and Processors User Manual" in chapter "Messaging Configuration Parameters":
https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=31007131_K01_000_16.pdf&p_Doc_Ref=31007131K01000

**Modicon Premium:**

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

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List following the recommendations of the user manual "Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual" in chapters "Connection configuration parameters / TCP/IP Services Configuration Parameters / Connection Configuration Parameters":
https://www.schneider-electric.com/en/download/document/35006192K01000/

**Modicon Quantum:**

Schneider Electric's Modicon 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 most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

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

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP
- Configure the Access Control List feature as mentioned in "Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual" in chapter

"Software Settings for Ethernet Communication / Messaging / Quantum NOE Ethernet Messaging Configuration":

https://www.schneider-electric.com/en/download/document/33002467K01000/

## Download Links

| M580 V2.90 Firmware | |
|---|---|
| BMEP584040 | https://www.schneider-https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV2.90/ |
| BMEH584040 and C | https://www.schneider-electric.com/en/download/document/M580_BMEH584040_SV2.90/ |
| BMEP586040 and C | https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV2.90/ |
| BMEH586040 and C | https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV2.90/ |
| BMEP581020 and H | https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV2.90/ |
| BMEP582020 and H | https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV2.90/ |
| BMEP582040 and H | https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV2.90/ |
| BMEP583020 | https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV2.90/ |
| BMEP583040 | https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV2.90/ |
| BMEP584020 | https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV2.90/ |
| BMEP585040 and C | https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV2.90/ |
| BMEH582040 and C | https://www.schneider-electric.com/en/download/document/M580_BMEH582040_SV2.90/ |

| | |
|---|---|
| BMEP584040S<br>BMEH584040S<br>BMEH586040S<br>BMEP582040S | Please contact Schneider Electric Support to receive the firmware version 2.90 |

| **M340 V3.10 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/ |

| **Control Expert Hot Fix V14.0** | |
|---|---|
| PMEPXM0100 EcoStruxure Control Expert Hot Fix V14.0 | https://www.schneider-electric.com/en/download/document/PMEPXM0100_Control_Expert_HF/ |

## 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 these vulnerabilities:

| CVE | Researcher(s) Name |
|---|---|
| CVE-2018-7842, CVE-2018-7843, CVE-2018-7844, CVE-2018-7845, CVE-2018-7846, CVE-2018-7847, CVE-2018-7848, CVE-2018-7849, CVE-2018-7850, CVE-2018-7852, CVE-2018-7853, CVE-2018-7854, CVE-2018-7855, CVE-2018-7856, CVE-2018-7857, CVE-2019-6806, CVE-2019-6807, CVE-2019-6808, CVE-2019-6809, CVE-2019-6828, CVE-2019-6829, CVE-2019-6830 | Jared Rittle (Cisco Talos) |

# Schneider Electric Security Notification

## 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



**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

### Revision Control:

| | |
|---|---|
| **Version 1**<br>*14 May 2019* | Original Release |
| **Version 1.1**<br>*9 Jul 2019* | Updated to include links to M580 V2.90 Firmware and Control Expert Hot Fix V14.0 |

# Schneider Electric Security Notification

| | |
|---|---|
| **Version 1.2**<br>*12 Jul 2019* | Updated mitigations for CVE-2019-6808 |
| **Version 1.3**<br>*24 Jul 2019* | Updated links to M580 V2.90 Firmware |
| **Version 2**<br>*13 Aug 2019* | Updated:<br>• CVE-2018-7846: added fix available for M340 V3.10<br>• CVE-2018-7849: added fix available for M340 V3.10<br>• CVE-2018-7848: added fix available for M340 V3.10<br>• CVE-2018-7842: added fix available for M340 V3.10<br>• CVE-2018-7847: added fix available for M340 V3.10<br>• CVE-2018-7850: added fix available for M340 V3.10<br>• CVE-2018-7854: added fix available for M340 V3.10<br>• CVE-2018-7852: modified to change M580 release which was erroneous (2.80 instead of 2.90)<br>• CVE-2018-7855: added fix available for M340 V3.10<br>• CVE-2019-6807: added fix available for M340 V3.10<br>• CVE-2019-6808: added fix available for M340 V3.10<br>• CVE-2018-7843: modified to change M340 release which was erroneous (3.01 instead of 3.10)<br>• CVE-2018-7856: added fix on M340 V3.10 (available earlier than expected)<br>Added 4 new CVEs:<br>• CVE-2019-6830<br>• CVE-2019-6828<br>• CVE-2019-6829<br>• CVE-2019-6809 |

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.12 11:10:50 -04'00'