Schneider Electric Security Notification

Security Notification – Modicon Controllers (V6.0)

14 May 2019 (08 December 2020)

Overview

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

December 2020 update: New fixes are available on Modicon M340 V3.30 to address an additional attack scenario related to CVE-2018-7857.

The Modicon Programmable Automation controllers are used for complex networked communication, display and control applications

Failure to apply the mitigations or remediations provided below may risk execution of unsolicited command on the PLC which could result in a loss of availability of the controller

Modicon M580 Remediation Steps & Download Links section

Modicon M340 Remediation Steps & Download Links section

Affected Products

- 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 V3.10, refer to the Remediation Steps & Download Links section.

- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20, please contact your Schneider Electric customer support to get the V3.20 firmware.

Modicon Quantum all versions prior to version V3.60 – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links section.

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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.

- **Modicon M340 all versions prior to V3.01** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20, please contact your Schneider Electric customer support to get the V3.20 firmware.
- **Modicon Quantum all versions prior to version V3.60** – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.01** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20; please contact your Schneider Electric customer support to get the V3.20 firmware.
- **Modicon Quantum all versions prior to version V3.60** – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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 V3.10, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20; please contact your Schneider Electric customer support to get the V3.20 firmware.

Modicon Quantum all versions prior to version V3.60 – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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 V2.90 or higher.
  - Fixes for additional attack scenarios are available in V3.10, refer to the Remediation Steps & Download Links section. Users are also encouraged to apply the additional recommendations proposed in the Mitigations section.
- **Modicon M340 all versions** – A partial fix is available for this vulnerability on Modicon M340 firmware V3.10 or higher.
  - December 2020 update: fixes for additional attack scenarios are available in V3.30, refer to the Remediation Steps & Download Links section. Users are also encouraged to apply the additional recommendations proposed 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-2019-6806**

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 variables in the controller using Modbus

Impacted versions:

- **Modicon M580 all firmware versions** – See recommendations in the Mitigations section
- **Modicon M340 all firmware 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-2019-6807**

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 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20, please contact your Schneider Electric customer support to get the V3.20 firmware.
- **Modicon Quantum all versions prior to version V3.60** – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20, please contact your Schneider Electric customer support to get the V3.20 firmware.
- **Modicon Quantum all versions prior to version V3.60** – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available

for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & 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 V3.10, refer to the Remediation Steps & Download Links section.
- **Modicon M340 with firmware version prior to V3.10** – A fix is available for this vulnerability on Modicon M340 firmware V3.20, refer to the Remediation Steps & Download Links section.
- **Modicon Premium all versions prior to version V3.20** – A fix is available on Modicon Premium V3.20; please contact your Schneider Electric customer support to get the V3.20 firmware.
- **Modicon Quantum all versions prior to version V3.60** – A fix is available on Modicon Quantum V3.60, links to fixed version in the Download links 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://www.se.com/ww/en/download/document/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.se.com/ww/en/download/document/HRB62665/

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://www.se.com/ww/en/download/document/31007131K01000/

Modicon Premium:

Schneider Electric's Modicon Premium 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 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.se.com/ww/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.se.com/ww/en/download/document/33002467K01000/

Remediation Steps & Download Links

M580 Remediation Steps

Schneider Electric has made a fix available via a free download. After downloading the fix, found in the below, all of the following steps are required to remediate the vulnerability:

STEP 1: Update software and firmware.

- On the engineering workstation, update to EcoStruxure Control Expert V14.1 (available below).
- On the Modicon M580 controller, update to firmware V3.10 or above, download link available below.

STEP 2: Update projects in Ecostruxure Control Expert by:

- Setting up an application password in the project properties
- Changing the version of the controller firmware to match the new firmware version of the target controller

STEP 3: Rebuild and transfer projects in EcoStruxure Control Expert:

- Rebuild all current projects
- Transfer them to Modicon controllers

M580 V3.10 Firmware	
BMEP584040	https://www.se.com/ww/en/download/document/M580_BMEP584040_SV3.10/
BMEH584040 and C	https://www.se.com/ww/en/download/document/M580_BMEH584040_SV3.10/
BMEP586040 and C	https://www.se.com/ww/en/download/document/M580_BMEP586040_SV3.10/

BMEH586040 and C	https://www.se.com/ww/en/download/document/M580_BMEH586040_SV3.10/
BMEP581020 and H	https://www.se.com/ww/en/download/document/M580_BMEP581020_SV3.10/
BMEP582020 and H	https://www.se.com/ww/en/download/document/M580_BMEP582020_SV3.10/
BMEP582040 and H	https://www.se.com/ww/en/download/document/M580_BMEP582040_SV3.10/
BMEP583020	https://www.se.com/ww/en/download/document/M580_BMEP583020_SV3.10/
BMEP583040	https://www.se.com/ww/en/download/document/M580_BMEP583040_SV3.10/
BMEP584020	https://www.se.com/ww/en/download/document/M580_BMEP584020_SV3.10/
BMEP585040 and C	https://www.se.com/ww/en/download/document/M580_BMEP585040_SV3.10/
BMEH582040 and C	https://www.se.com/ww/en/download/document/M580_BMEH582040_SV3.10/
BMEP584040S	https://www.se.com/ww/en/download/document/M580_BMEP584040S_SV3.10/
BMEH584040S	https://www.se.com/ww/en/download/document/M580_BMEH584040S_SV3.10/
BMEH586040S	https://www.se.com/ww/en/download/document/M580_BMEH586040S_SV3.10/
BMEP582040S	https://www.se.com/ww/en/download/document/M580_BMEP582040S_SV3.10/

M340 Remediation Steps

Schneider Electric has made a fix available via a free download. After downloading the fix, found below, all of the following steps are required to remediate the vulnerability:

STEP 1: Update software and firmware.

- On the engineering workstation, update to EcoStruxure Control Expert V14.1 (available below).
- On the Modicon M340 controller, update to firmware V3.30 or above, download link available below.

STEP 2: Update projects in Ecostruxure Control Expert by:

- Setting up an application password in the project properties
- Changing the version of the controller firmware to match the new firmware version of the target controller

STEP 3: Rebuild and transfer projects in EcoStruxure Control Expert:

- Rebuild all current projects
- Transfer them to Modicon controllers

M340 V3.30 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

Premium V3.20 firmware	
TSXP57104M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57154M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP571634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57204M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP572634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57254M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57304M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.

TSXP573634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57354M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP574634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57454M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP575634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP57554M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXP576634M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXH5724M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.
TSXH5744M [C]	Please contact your Schneider Electric customer support to get Premium V3.20 firmware.

Quantum V3.60 firmware

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
140CPU65160S	Please contact your Schneider Electric customer support to get Quantum V3.60 firmware
140CPU67160S	Please contact your Schneider Electric customer support to get Quantum V3.60 firmware

EcoStruxure™ Control Expert
hhttps://www.se.com/ww/en/product-range-download/548-ecostruxure%E2%84%A2-control-expert/?parent-subcategory-id=3950&filter=business-1-industrial-automation-and-control#/software-firmware-tab

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 the following industry cybersecurity best practices:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.

- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are 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-2018-7843, CVE-2018-7844, CVE-2018-7845, CVE-2018-7850, CVE-2018-7852, CVE-2018-7853, CVE-2018-7854, CVE-2018-7855, CVE-2018-7856, 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)
CVE-2018-7842, CVE-2018-7846, CVE-2018-7847, CVE-2018-7848, CVE-2018-7849	Jared Rittle (Cisco Talos) Pavel Nesterov and Artem Zinenko from Kaspersky ICS CERT
CVE-2018-7857	Jared Rittle (Cisco Talos) Dong Yang (Dingxiang Dongjian Security Lab) Gao Jian (ns focus)

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

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

https://www.se.com/ww/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 1.0 *14 May 2019*	Original Release
Version 1.1 *9 Jul 2019*	Updated to include links to M580 V2.90 Firmware and Control Expert Hot Fix V14.0
Version 1.2 *12 Jul 2019*	Updated mitigations for CVE-2019-6808
Version 1.3 *24 Jul 2019*	Updated links to M580 V2.90 Firmware
Version 2.0 *13 Aug 2019*	Updated: ○ CVE-2018-7846: added fix available for M340 V3.10 ○ CVE-2018-7849: added fix available for M340 V3.10 ○ CVE-2018-7848: added fix available for M340 V3.10 ○ CVE-2018-7842: added fix available for M340 V3.10

	○ CVE-2018-7847: added fix available for M340 V3.10 ○ CVE-2018-7850: added fix available for M340 V3.10 ○ CVE-2018-7854: added fix available for M340 V3.10 ○ CVE-2018-7852: modified to change M580 release which was erroneous (2.80 instead of 2.90) ○ CVE-2018-7855: added fix available for M340 V3.10 ○ CVE-2019-6807: added fix available for M340 V3.10 ○ CVE-2019-6808: added fix available for M340 V3.10 ○ CVE-2018-7843: modified to change M340 release which was erroneous (3.01 instead of 3.10) ○ CVE-2018-7856: added fix on M340 V3.10 (available earlier than expected) Added 4 new CVEs: ○ CVE-2019-6830 ○ CVE-2019-6828 ○ CVE-2019-6829 ○ CVE-2019-6809
Version 3.0 *10 Dec 2019*	Updated: ○ CVE-2019-6806: Corrected remediation information for Modicon M340 ○ CVE-2018-7845: Fix for Premium & Quantum ○ CVE-2018-7843: Fix for Premium & Quantum ○ CVE-2019-6809: Fix for Premium & Quantum ○ CVE-2019-6807: Fix for Premium & Quantum ○ CVE-2018-7857: Fix for Premium & Quantum ○ CVE-2018-7856: Fix for Premium & Quantum ○ CVE-2018-7852: Fix for Premium & Quantum ○ CVE-2019-6828: Fix for Premium & Quantum ○ Update of download links for latest versions of M580 / M340 & Quantum, plus customer support information for Premium.
Version 4.0 *12 May 2020*	Updated fix version information for CVE-2018-7857
Version 4.1 *11 August 2020*	Updated fix version information for CVE-2018-7857: ○ Additional fixes available for M580 v3.10 ○ Quantum & Premium previous fix is not enough to correct the CVE and requires the additional mitigations proposed
Version 5.0 *12 October 2020*	Additional required remediation steps added for M580 and M340 applicable to the following CVEs: • CVE-2018-7846 • CVE-2018-7849 • CVE-2018-7843 • CVE-2018-7848

	• CVE-2018-7842 • CVE-2018-7847 • CVE-2018-7850 • CVE-2018-7845 • CVE-2018-7852 • CVE-2018-7853 • CVE-2018-7854 • CVE-2018-7855 • CVE-2018-7856 • CVE-2018-7857 • CVE-2019-6807 • CVE-2019-6808 • CVE-2019-6830 • CVE-2019-6828 • CVE-2019-6829 • CVE-2019-6809
Version 6.0 *8 December 2020*	A fix for additional attack scenario is available on M340 V3.30 for CVE-2018-7857

Product Security Office

Digitally signed by Product Security Office
Date: 2020.12.06 14:08:13 -05'00'