

# Schneider Electric Security Notification

## Modicon Controllers

14 May 2019 (11 February 2025)

### Overview

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

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

**February 2025 Update:** Correction of vulnerabilities impacting Quantum Safety processor.

### Affected Products

- Modicon M580
- Modicon M340
- Modicon MC80
- Modicon Momentum Unity M1E Processor (part numbers 171CBU\*)
- Modicon Quantum
- Modicon Quantum Safety
- Modicon Premium
- PLC Simulator for EcoStruxure™ Control Expert

### 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

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, 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 v3.10, refer to the [Remediation Steps & Download Links section](#).

## Schneider Electric Security Notification

- **Modicon Premium all versions** – See recommendations in the [Mitigations section](#).
- **Modicon Quantum all versions** – See recommendations in the [Mitigations section](#).
- **Modicon Quantum Safety 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

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 v2.90, 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 v3.10, 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](#).
- **Modicon Quantum Safety 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

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 v3.10, 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](#).

## 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

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, 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 v3.10, 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](#).
- **Modicon Quantum Safety 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

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, 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 v3.10, 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](#).
- **Modicon Quantum Safety 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

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.

## Schneider Electric Security Notification

Impacted versions:

- **Modicon M580 with firmware version prior to v2.90** – A fix is available for this vulnerability on Modicon M580 firmware v2.90, 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 v3.10, 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](#)
- **Modicon Quantum Safety 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

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, 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 v3.10, 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](#)
- **Modicon Quantum Safety 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

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, refer to the [Remediation Steps & Download Links section](#).

## Schneider Electric Security Notification

- **Modicon M340 all versions prior to v3.01** – A fix is available for this vulnerability on Modicon M340 firmware v3.01, 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

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, 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 v3.01, 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](#).
- **Modicon Quantum Safety all versions** – 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

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, 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

## Schneider Electric Security Notification

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, 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 v3.10, 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

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 Premium all versions** – See recommendations in the [Mitigations section](#)
- **Modicon Quantum all versions** – See recommendations in the [Mitigations section](#)
- **Modicon Quantum Safety all versions** – See recommendations in the [Mitigations section](#)
- **Modicon M580 firmware version prior to v4.20** – A fix is available for this vulnerability on Modicon M580 firmware v4.20, refer to the [Remediation Steps & Download Links section](#).
- **Modicon M340 firmware version prior to v3.60** – A fix is available for this vulnerability on Modicon M340 firmware v3.60, refer to the [Remediation Steps & Download Links section](#).
- **Modicon MC80 all versions** – See recommendations in the [Mitigation section](#)
- **Modicon Momentum M1E 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

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, refer to the [Remediation Steps & Download Links section](#).

## Schneider Electric Security Notification

- **Modicon M340 with firmware version prior to v3.10** – A fix is available for this vulnerability on Modicon M340 firmware v3.10, 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

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.
  - 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](#)
- **Modicon Quantum Safety all versions** – See recommendations in the [Mitigations section](#)
- **Modicon MC80 firmware version prior to v1.80** – A fix is available for this vulnerability on Modicon MC80 (part numbers BMKC80\*), refer to the [Remediation Steps & Download Links section](#).
- **Modicon Momentum CPU (part numbers 171CBU\*) all versions** – See recommendations in the [Mitigations section](#)
- **PLC Simulator for EcoStruxure™ Control Expert prior to v15.1** – A fix is available for this vulnerability on PLC Simulator, refer to the [Remediation Steps & Download Links section](#).
- **Modicon Momentum Unity M1E Processor (part numbers 171CBU\*) versions prior to sv2.6** – A fix is available for this vulnerability on Modicon Momentum CPU, refer to the [Remediation Steps & Download Links section](#).

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



## Schneider Electric Security Notification

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

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](#)
- **Modicon Quantum Safety 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

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, 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 v3.10, 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](#).
- **Modicon MC80 with firmware version prior to v1.80** – A fix is available for this vulnerability on Modicon MC80 (part numbers BMKC80\*), refer to the [Remediation Steps & Download Links section](#).
- **Modicon Momentum CPU (part numbers 171CBU\*) all versions** – See recommendations in the [Mitigations section](#)
- **PLC Simulator for EcoStruxure™ Control Expert prior to v15.1** – A fix is available for this vulnerability on PLC Simulator, refer to the [Remediation Steps & Download Links section](#).
- **Modicon Momentum Unity M1E Processor (part numbers 171CBU\*) versions prior to sv2.6** – A fix is available for this vulnerability on Modicon Momentum CPU, refer to the [Remediation Steps & Download Links section](#).

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



## Schneider Electric Security Notification

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

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, 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 v3.10, 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](#).
- **Modicon Quantum Safety 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

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](#).
- **Modicon Quantum Safety 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

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, 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

## Schneider Electric Security Notification

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, 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 v3.10, 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

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, 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 v3.10, 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

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, 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 v3.10, 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.

## Schneider Electric Security Notification

- **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:

It is recommended to apply the following mitigations to reduce the risk of the exploit:

- Setup an application password in the project properties
- 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 manuals:
  - “Modicon M580, Hardware, Reference Manual”:  
<https://www.se.com/ww/en/download/document/EIO0000001578/>
- 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 Schneider Electric Security Notification Module, Installation and Configuration Guide” in the chapter “Configuring IPSEC communications”:  
<https://www.se.com/ww/en/download/document/HRB62665/>

#### OR

- 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>

#### OR

- Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections for M340 and M580 architectures. For more details refer to the chapter “How to protect M580 and M340 architectures with EAGLE40 using VPN”: <https://www.se.com/ww/en/download/document/EIO0000001999/>
- Ensure the M580 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

## Schneider Electric Security Notification

Memory Protection section”:

<https://www.schneider-electric.com/en/download/document/EIO0000001999/>

- NOTE: The CPU memory protection cannot be configured with M580 Hot Standby CPUs. In such cases, use IPsec encrypted communication.

### **Modicon M340:**

It is recommended to apply the following mitigations to reduce the risk of the exploit:

- Setup an application password in the project properties
- 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 manuals:
  - “Modicon M340 for Ethernet Communications Modules and Processors User Manual” in chapter “Messaging Configuration Parameters”:  
<https://www.se.com/ww/en/download/document/31007131K01000/>
- 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/>
- Consider use of external firewall devices such as EAGLE40-07 from Belden to establish VPN connections for M340 & M580 architectures. For more details refer to the chapter “How to protect M580 and M340 architectures with EAGLE40 using VPN”: <https://www.se.com/ww/en/download/document/EIO0000001999/>

### **Modicon Momentum:**

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

- Setup an application password in the project properties
- 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 manuals:
  - “Momentum for EcoStruxure™ Control Expert - 171 CBU 78090, 171 CBU 98090, 171 CBU 98091 Processors” manual in the chapter “Modbus Messaging and Access Control” [https://download.schneider-electric.com/files?p\\_enDocType=User+guide&p\\_File\\_Name=HRB44124.08.pdf&p\\_Doc\\_Ref=HRB44124](https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=HRB44124.08.pdf&p_Doc_Ref=HRB44124)
- Setup a secure communication according to the following guideline “Modicon Controller Systems Cybersecurity, User Guide” in chapter “Set Up Encrypted Communication”: <https://www.se.com/ww/en/download/document/EIO0000001999/>

## Schneider Electric Security Notification

- Setup a VPN between the Modicon PLC controllers and the engineering workstation containing EcoStruxure Control Expert or Process Expert. Note: this functionality may be provided by an external IPSEC compatible firewall located close to the controller.

### **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 & Quantum Safety:**

Schneider Electric's Modicon Quantum and Quantum Safety controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon M580 or M580 Safety 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/>

### **Modicon MC80:**

To mitigate the risks associated with CVE-2018-7855, users should immediately apply the following steps:

- Setup an application password in the project properties

## Schneider Electric Security Notification

- 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 manuals:
- “Modicon MC80 Programmable Logic Controller (PLC) manual” in the chapter “Access Control List (ACL)”: <https://www.se.com/ww/en/download/document/EIO0000002071/>
- Setup a secure communication according to the following guideline “Modicon Controller Systems Cybersecurity, User Guide” in chapter “Set Up Encrypted Communication”: <https://www.se.com/ww/en/download/document/EIO0000001999/>

### **PLC Simulator for EcoStruxure™ Control Expert**

Customers should immediately apply the following mitigations to reduce the risk of exploit:

- On the engineering workstation, update to EcoStruxure Control Expert v15.1 or later (<https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware>).
- Ensure to use simulator default panel option to make PLC simulator accessible only locally.
- Modbus network connections are disabled by default on the PLC Simulator present in EcoStruxure™ Control Expert, mitigating the risk associated to this vulnerability.

Note: The PLC Simulator feature is part of the EcoStruxure Control Expert software, and it helps users to review and test their configurations files in a simulation environment. It is not intended to be used as a controller CPU in a production environment.

## 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 v16.0(<https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/-software-and-firmware>).
- On the Modicon M580 controller, update to firmware SV4.20 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

## Schneider Electric Security Notification

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

- Rebuild all current projects
- Transfer them to Modicon controllers

M580 sv4.20 Firmware	
<b>Modicon M580 (part numbers BMEP* and BMEH*, excluding M580 CPU Safety)</b> <i>Versions prior to sv4.20</i>	<a href="https://www.se.com/ww/en/product-range/62098-modicon-m580-epac/#software-and-firmware">https://www.se.com/ww/en/product-range/62098-modicon-m580-epac/#software-and-firmware</a>

### 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 v16.0 or later (<https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware>).
- On the Modicon M340 controller, update to firmware v3.60 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 SV3.60 Firmware	
<b>Modicon M340 CPU (part numbers BMXP34*)</b> <i>Versions prior to sv3.60</i>	<a href="https://www.se.com/ww/en/product-range/1468-modicon-m340/#software-and-firmware">https://www.se.com/ww/en/product-range/1468-modicon-m340/#software-and-firmware</a>



## Schneider Electric Security Notification

### **Modicon MC80 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 V15.1 or later (<https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware>).
- On the Modicon MC80 controller, update to firmware V1.80 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

MC80 v1.80 Firmware	
BMKC8020301	<a href="https://www.se.com/ww/en/product-range/62396-modicon-mc80/#software-and-firmware">https://www.se.com/ww/en/product-range/62396-modicon-mc80/#software-and-firmware</a>

### **Modicon Momentum Unity M1E Processor (part numbers 171CBU\*) 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 v15.1 or later (<https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware>).
- On the Modicon Momentum CPU, update to firmware v2.6, 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

## Schneider Electric Security Notification

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

- Rebuild all current projects
- Transfer them to Modicon controllers

Modicon Momentum CPU sv2.6 Firmware	
171CBU98090	<a href="https://www.se.com/ww/en/download/document/Momentum_FW_update/">https://www.se.com/ww/en/download/document/Momentum_FW_update/</a>

### Premium v3.20 firmware

Premium v3.20 firmware	
TSXP57104M [C] TSXP57154M [C] TSXP571634M [C] TSXP57204M [C] TSXP572634M [C] TSXP57254M [C] TSXP57304M [C] TSXP573634M [C] TSXP57354M [C] TSXP574634M [C] TSXP57454M [C] TSXP575634M [C] TSXP57554M [C] TSXP576634M [C] TSXH5724M [C] TSXH5744M [C]	<p>Please contact your <a href="#">Schneider Electric customer support</a> to get Premium V3.20 firmware.</p>

### Quantum v3.60 firmware

Quantum v3.60 firmware	
140CPU65150 [C] 140CPU65160 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU651X0_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU651X0_SV3.60</a>
140CPU65260 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU65260_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU65260_SV3.60</a>
140CPU67261 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60</a>
140CPU67060 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67060_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67060_SV3.60</a>

## Schneider Electric Security Notification

140CPU67160 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67160_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67160_SV3.60</a>
140CPU67261 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67261_SV3.60</a>
140CPU67260 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67260_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67260_SV3.60</a>
140CPU65860 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU65860_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU65860_SV3.60</a>
140CPU67861 [C]	<a href="https://www.schneider-electric.com/en/download/document/Quantum_140CPU67861_SV3.60">https://www.schneider-electric.com/en/download/document/Quantum_140CPU67861_SV3.60</a>

### **PLC Simulator for EcoStruxure™ Control Expert**

Schneider Electric has made a fix available via a free download.

<b>EcoStruxure™ Control Expert v15.1</b>
<a href="https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware">https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#software-and-firmware</a>

## 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](http://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:

## Schneider Electric Security Notification

- 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 researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers 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) Gao Jian (ns focus)
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)

# 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 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>

<https://www.se.com/ww/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

Schneider's purpose is to **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

[www.se.com](http://www.se.com)

## Revision Control:

## Schneider Electric Security Notification

<b>Version 1.0.0</b> 14 May 2019	Original Release
<b>Version 1.1.0</b> 09 Jul 2019	Updated to include links to M580 V2.90 Firmware and Control Expert Hot Fix v14.0
<b>Version 1.2.0</b> 12 Jul 2019	Updated mitigations for CVE-2019-6808
<b>Version 1.3.0</b> 24 Jul 2019	Updated links to M580 v2.90 Firmware
<b>Version 2.0.0</b> 13 Aug 2019	<p>Updated:</p> <ul style="list-style-type: none"> <li>• CVE-2018-7846: added fix available for M340 v3.10</li> <li>• CVE-2018-7849: added fix available for M340 v3.10</li> <li>• CVE-2018-7848: added fix available for M340 v3.10</li> <li>• CVE-2018-7842: added fix available for M340 v3.10</li> <li>• CVE-2018-7847: added fix available for M340 v3.10</li> <li>• CVE-2018-7850: added fix available for M340 v3.10</li> <li>• CVE-2018-7854: added fix available for M340 v3.10</li> <li>• CVE-2018-7852: modified to change M580 release which was erroneous (2.80 instead of 2.90)</li> <li>• CVE-2018-7855: added fix available for M340 v3.10</li> <li>• CVE-2019-6807: added fix available for M340 v3.10</li> <li>• CVE-2019-6808: added fix available for M340 V3.10</li> <li>• CVE-2018-7843: modified to change M340 release which was erroneous (3.01 instead of 3.10)</li> <li>• CVE-2018-7856: added fix on M340 v3.10 (available earlier than expected)</li> </ul> <p>Added 4 new CVEs:</p> <ul style="list-style-type: none"> <li>• CVE-2019-6830</li> <li>• CVE-2019-6828</li> <li>• CVE-2019-6829</li> <li>• CVE-2019-6809</li> </ul>

## Schneider Electric Security Notification

<p><b>Version 3.0.0</b> 10 Dec 2019</p>	<p>Updated:</p> <ul style="list-style-type: none"> <li>• CVE-2019-6806: Corrected remediation information for Modicon M340</li> <li>• CVE-2018-7845: Fix for Premium &amp; Quantum</li> <li>• CVE-2018-7843: Fix for Premium &amp; Quantum</li> <li>• CVE-2019-6809: Fix for Premium &amp; Quantum</li> <li>• CVE-2019-6807: Fix for Premium &amp; Quantum</li> <li>• CVE-2018-7857: Fix for Premium &amp; Quantum</li> <li>• CVE-2018-7856: Fix for Premium &amp; Quantum</li> <li>• CVE-2018-7852: Fix for Premium &amp; Quantum</li> <li>• CVE-2019-6828: Fix for Premium &amp; Quantum</li> <li>• Update of download links for latest versions of M580 / M340 &amp; Quantum, plus customer support information for Premium.</li> </ul>
<p><b>Version 4.0.0</b> 12 May 2020</p>	<p>Updated fix version information for CVE-2018-7857</p>
<p><b>Version 4.1.0</b> 11 August 2020</p>	<p>Updated fix version information for CVE-2018-7857:</p> <ul style="list-style-type: none"> <li>• Additional fixes available for M580 v3.10</li> <li>• Quantum &amp; Premium previous fix is not enough to correct the CVE and requires the additional mitigations proposed</li> </ul>
<p><b>Version 5.0.0</b> 12 October 2020</p>	<p>Additional required remediation steps added for M580 and M340 applicable to the following CVEs:</p> <ul style="list-style-type: none"> <li>• CVE-2018-7846</li> <li>• CVE-2018-7849</li> <li>• CVE-2018-7843</li> <li>• CVE-2018-7848</li> <li>• CVE-2018-7842</li> <li>• CVE-2018-7847</li> <li>• CVE-2018-7850</li> <li>• CVE-2018-7845</li> <li>• CVE-2018-7852</li> <li>• CVE-2018-7853</li> <li>• CVE-2018-7854</li> <li>• CVE-2018-7855</li> <li>• CVE-2018-7856</li> <li>• CVE-2018-7857</li> <li>• CVE-2019-6807</li> <li>• CVE-2019-6808</li> <li>• CVE-2019-6830</li> <li>• CVE-2019-6828</li> <li>• CVE-2019-6829</li> <li>• CVE-2019-6809</li> </ul>



## Schneider Electric Security Notification

<b>Version 6.0.0</b> <i>08 December 2020</i>	A fix for additional attack scenario is available on M340 v3.30 for CVE-2018-7857.
<b>Version 7.0.0</b> <i>13 September 2022</i>	Modicon MC80 and PLC Simulator for EcoStruxure™ Control Expert were added as impacted product of CVE-2018-7857 and CVE-2019-6807 and the remediation is provided.
<b>Version 8.0.0</b> <i>10 January 2023</i>	Modicon M340 and M580 latest firmware versions are affected by CVE-2018-7855 and additional mitigations were added in the mitigation section.
<b>Version 9.0.0</b> <i>14 March 2023</i>	A remediation is available for Modicon Momentum Unity M1E Processor part numbers 171CBU* for CVE-2018-7857 and CVE-2019-6807
<b>Version 10.0.0</b> <i>13 February 2024</i>	A remediation is available for Modicon M340 and M580 for CVE-2018-7855. Updated products affected version numbers.
<b>Version 11.0.0</b> <i>09 July 2024</i>	Modicon MC80 and Momentum M1E PLCs were added as impacted products of CVE-2018-7855. Mitigations are available for Modicon MC80 and Momentum M1E PLCs for CVE-2018-7855.
<b>Version 12.0.0</b> <i>11 Feb 2025</i>	Correction of CVE list impacting Quantum Safety processor.