# Schneider Electric Security Notification

## Modicon M218 Logic Controller

**9 June 2020**

## Overview

Schneider Electric is aware of a vulnerability in the Modicon M218 Logic Controller product.

## Affected Product(s)

Modicon M218 firmware version 4.3 and prior

## Vulnerability Details

CVE ID: **CVE-2020-7502**

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-787: Out-of-bounds Write vulnerability exists, which may cause a Denial of Service when specific TCP/IP crafted packets are sent to the Modicon M218 Logic Controller.

## Remediation

The following workarounds and mitigations can be applied by customers to reduce the risk:

Since the vulnerability is present in the TCP/IP stack of the Modicon M218 Logic Controller product, an active network connection is required to exploit it. Therefore, Schneider Electric customers can act now to mitigate the risk of attack by limiting access to their devices, which would immediately reduce attempted exploits:

- Limit access to the networks on which Schneider Electric devices are placed.
- Do not expose Schneider Electric devices directly to the Internet.
- Always place Schneider Electric devices behind firewalls and/or other security protection appliances that limit access only to authorized remote connections.
- Continuously monitor affected devices for security events that could warn of attempted unauthorized access.
- Secure the network communications between the engineering workstation and the controllers to ensure trustworthiness by following the Cybersecurity Best Practices https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/

# Schneider Electric Security Notification

For more details and assistance on how to protect your installation, please contact your local Schneider Electric's Industrial Cybersecurity Services organization.

This notification will be updated as remediation become available with a dedicated patch fixing the vulnerability.

## Product Information

**Modicon M218** is a Programmable Logic Controller (PLC), used to manage equipment in plants and on assembly lines, allowing for digitized control over precise robotic or mechanical actions. Modicon PLC controls and monitors industrial operations in a way that is sustainable, efficient, and flexible.

**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**

Customers using Modicon M218 Logic Controller with firmware version 4.3 or prior are affected.

## 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.
- 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 for.
- 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.

# Schneider Electric Security Notification

## Acknowledgments

Schneider Electric thanks CNCERT for helping to coordinate a response to this vulnerability.

## 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.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

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



### About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

# Schneider Electric Security Notification

Revision Control:

| | |
|---|---|
| **Version 1**<br>*9 June 2020* | Original Release |

## Product Security Office

Digitally signed by Product Security Office
Date: 2020.06.07 14:09:28 -04'00'