

# Schneider Electric Security Notification

## Modicon LMC078 Logic Controller additional URGENT/11 Fix

9 June 2020

### Overview

Schneider Electric is aware of a vulnerability introduced in the VxWorks patch delivered by Wind River fixing URGENT/11 vulnerabilities affecting the Modicon LMC078 Logic Controller.

### Affected Product(s)

Modicon LMC078 Logic Controller running with firmware version V1.51.15.05 and later

### Vulnerability Details

CVE ID: **CVE-2020-10664**

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

The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.

Additional details on this specific vulnerability can be found on the Wind River security notification webpage: <https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-10664>

### Remediation

Modicon LMC078 Logic Controller does not allow IGMP communication protocol by default.

No configuration or Schneider feature allows joining a multicast source group.

The following workarounds and mitigations can be applied by customers to enforce cybersecurity on Modicon LMC078 Logic Controllers:

Since the vulnerability is present in the TCP/IP stack, 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.

## Schneider Electric Security Notification

- Use functions recommended and documented by Schneider Electric:  
[https://product-help.schneider-electric.com/Machine%20Expert/V1.2/LandingPages/en/VLP\\_Software/VLP\\_Lib\\_Template\\_Ex/VLP\\_Libraries/VLP\\_Communication\\_Libraries/index.html](https://product-help.schneider-electric.com/Machine%20Expert/V1.2/LandingPages/en/VLP_Software/VLP_Lib_Template_Ex/VLP_Libraries/VLP_Communication_Libraries/index.html)
- 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 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/>

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

### Product Information

**Modicon LMC078** 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: <https://www.se.com/us/en/all-products>

#### How to determine if you are affected

Customers using Modicon LMC078 Logic Controller with firmware version V1.51.15.05 and later are affected.

### 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.

## Schneider Electric Security Notification

- 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.

### 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>

#### 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.

# Schneider Electric Security Notification

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

Revision Control:

<p><b>Version 1</b> 9 June 2020</p>	<p>Original Release</p>
---	-------------------------