Schneider Electric Security Notification

PowerLogic PM5300 Series

12 November 2024

Overview

Schneider Electric is aware of a vulnerability in its PowerLogic PM5300 series with ethernet functionality.

PowerLogic PM5300 series offers a compact, versatile power meter for energy cost and basic network management applications.

Failure to apply the remediation below may risk loss of communication to the device leading to a denial of service.

Affected Products and Versions

Product	Version
PowerLogic PM5320	Version 2.3.8 and prior
PowerLogic PM5340	Version 2.3.8 and prior
PowerLogic PM5341	Version 2.6.6 and prior

Note – PM5310 and PM5330 are not impacted because they use serial communication infrastructure and do not have an Ethernet stack.

Vulnerability Details

CVE ID: **CVE-2024-9409**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-400: An Uncontrolled Resource Consumption vulnerability exists that could cause the device to become unresponsive resulting in communication loss when a large amount of IGMP packets is present in the network.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 (CVSS v4.0). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

Affected Product & Version	Remediation
PowerLogic PM5320 *Version 2.3.8 and prior*	Version 2.4.0 of PowerLogic PM5320 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/METSEPM5320/power-meter-powerlogic-pm5320-ethernet-up-to-31st-harmonic-256kb-2di-2do-35-alarms/
PowerLogic PM5340 *Version 2.3.8 and prior*	Version 2.4.0 of PowerLogic PM5340 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/METSEPM5340/power-meter-powerlogic-pm5340-ethernet-up-to-31st-harmonic-256kb-2di-2do-35-alarms/
PowerLogic PM5341 *Version 2.6.6 and prior*	Version 2.7.0 of PowerLogic PM5341 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/METSEPM5341/pm5341-meter-ethernet-up-to-31st-h-256k-2di-2do-35-alarms-mid/

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following steps to reduce the risk of exploit:

1. Enable IGMP Snooping:
    - Ensure that IGMP Snooping is enabled on the switch. This feature allows the switch to intelligently forward multicast traffic only to the necessary ports where interested hosts reside. It prevents unnecessary flooding of multicast traffic across all ports, thereby enhancing network efficiency and minimizing unnecessary load on network resources.
2. Configure VLAN Interface Settings:
    - Set up VLAN interface settings on the switch. It's important to have distinct configurations for each VLAN to ensure proper IGMP operation.
3. Multicast Filtering:
    - Use IGMP filtering to control the propagation of IGMP traffic through the network. This involves configuring filters on a switch virtual interface (SVI), per-port, or per-port per-VLAN basis. Multicast filtering helps manage IGMP snooping and controls multicast traffic forwarding effectively.

Schneider Electric Security Notification

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 intended for that device.
- 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 mobile devices 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 refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, visit the company’s cybersecurity support portal page: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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

Revision Control:

Version 1.0.0 *12 November 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.11.11 10:54:14 -05'00'