

Schneider Electric Security Notification

PowerLogic PM5500 and PowerLogic PM8ECC

8 June 2021 (12 November 2024)

Overview

Schneider Electric is aware of a vulnerability in its PowerLogic PM55xx and PowerLogic PM8ECC products.

The PowerLogic [PM55xx](#) products are power metering devices. The PowerLogic [PM8ECC](#) product is an ethernet communication module.

Failure to apply the mitigations or remediations provided below may risk elevation of privileges, which could result in loss of control of the affected device.

Update November 2024: Remediation is now available for PM5562.

Affected Products and Versions

CVE	Product	Version
CVE-2021-22763 CVE-2021-22764	PM5560	Versions prior to v2.7.8
	PM5561	Versions prior to v10.7.3
	PM5562	v2.5.4 and prior
	PM5563	Versions prior to v2.7.8
CVE-2021-22763	PM8ECC	All versions

Vulnerability Details

CVE ID: **CVE-2021-22763**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could allow an attacker administrator level access to a device.

CVE ID: **CVE-2021-22764**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CWE-287: Improper Authentication vulnerability exists that could cause loss of connectivity to the device via Modbus TCP protocol when an attacker sends a specially crafted HTTP request.

Schneider Electric Security Notification

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 ([CVSS v3.1](#)) 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

Product	Version	Remediation
PM5560	Versions prior to v2.7.8	<p>Version 2.8.3 of the PowerLogic PM5560, 5563, 5580 firmware includes fixes for these vulnerabilities. The version update files are available for download here:</p> <p>https://www.se.com/ww/en/product-range/61281-powerlogic-pm5000-power-meters/?parent-subcategory-id=4125&filter=business-2-building-automation-and-control-software-and-firmware</p>
PM5563	Versions prior to v2.7.8	<p>If customers choose not to apply the remediation provided above, they should immediately apply the following mitigation to reduce the risk of exploit:</p> <p>Customers should consider blocking HTTP access to the device at the firewall level or disable the HTTP web service to reduce the risk of exposure.</p>
PM5561	Versions prior to v10.7.3	<p>Version 10.7.3 of the PowerLogic PM5561 firmware includes fixes for these vulnerabilities. The version update files are available for download here:</p> <p>https://www.se.com/ww/en/product-range/61281-powerlogic-pm5000-power-meters/?parent-subcategory-id=4125&filter=business-2-building-automation-and-control#software-and-firmware</p> <p>If customers choose not to apply the remediation provided above, they should immediately apply the following mitigation to reduce the risk of exploit:</p> <p>Customers should consider blocking HTTP access to the device at the firewall level or disable the HTTP web service to reduce the risk of exposure.</p>

Schneider Electric Security Notification

PM5562	Versions prior to v4.3.5	<p>Version 4.3.5 of the PowerLogic PM5562 firmware includes fixes for these vulnerabilities. The version update files are available for download here: https://www.se.com/ww/en/product-range/61281-powerlogic-pm5000/12146169702-basic-multifunction-metering/?selected-node-id=12146169702&N=brand=se%26country-code=UK%26language-code=en%26node-id=12146169702-software-and-firmware</p> <p>If customers choose not to apply the remediation provided above, they should immediately apply the following mitigation to reduce the risk of exploit:</p> <p>Customers should consider blocking HTTP access to the device at the firewall level or disable the HTTP web service to reduce the risk of exposure.</p>
PM8ECC	All versions	<p>PowerLogic PM8ECC has reached end of service and is no longer supported. Customers should immediately apply the following mitigation to reduce the risk of exploit:</p> <p>Customers should consider blocking HTTP access to the device at the firewall level once commissioning is complete to reduce the risk of exposure. Additionally, Customers should ensure the General security Recommendations listed below are in place.</p>

Note: There may be newer versions of the firmware available for download, please check se.com before upgrading.

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.

Schneider Electric Security Notification

- 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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2021-22763 CVE-2021-22764	Jacob Baines (Dragos)

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>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN 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 Electric Security Notification

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 <i>08 June 2021</i>	Original Release
Version 2.0.0 <i>12 November 2024</i>	Remediation now available for PM5562.