

Schneider Electric Security Notification

PowerLogic™ HDPM6000 High-Density Metering System

14 January 2025

Overview

Schneider Electric is aware of multiple vulnerabilities in its PowerLogic™ HDPM6000 High-Density Metering System product.

The [HDPM6000](#) products are high-density, multi-circuit busway and panelboard power meters for cost and network management in large and critical power applications.

Failure to apply the remediation provided below may risk a low privileged user gaining higher level access, which could allow for modification of system configuration parameters or an unauthenticated user causing data corruption or denial of service to the devices web interface via a specially crafted Modbus protocol write operation.

Affected Products and Versions

Product	CVE-2024-10497	CVE-2024-10498
PowerLogic™ HDPM6000	Version v0.62.7 only	Versions v0.62.7 and prior

Vulnerability Details

CVE ID: **CVE-2024-10497**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-639: Authorization Bypass Through User-Controlled Key vulnerability exists that could allow an authorized attacker to modify values outside those defined by their privileges (Elevation of Privileges) when the attacker sends modified HTTPS requests to the device.

CVE ID: **CVE-2024-10498**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v4.0 Base Score 6.9 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could allow an unauthorized attacker to modify configuration values outside of the normal range when the attacker sends specific Modbus write packets to the device which could result in invalid data or loss of web interface functionality.

Schneider Electric Security Notification

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	CVE	Remediation
PowerLogic™ HDPM6000 Version v0.62.7 only	CVE-2024-10497	Version v0.62.11 and newer of HDPM6000 includes a fix for these vulnerabilities and is available for download here: <ul style="list-style-type: none">https://www.se.com/ww/en/product-range/8297113-powerlogic-hdpm6000/-software-and-firmwareA device restart will occur as part of the firmware update process if conducted through the web user interface. If the upgrade is performed using the HDPM6000 Manager software, the device will need to be restarted manually to apply the update.
PowerLogic™ HDPM6000 Versions v0.62.7 and prior	CVE-2024-10498	

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 mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	CVE	Mitigation
PowerLogic™ HDPM6000 Version v0.62.7 only	CVE-2024-10497	If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit: <ul style="list-style-type: none">Ensure that the device is not accessible via the HTTPS protocol outside the local network segment by applying appropriate firewalls configuration and controls, and that access to the network segment is protected and controlled.
HDPM6000 Versions v0.62.7 and prior	CVE-2024-10498	If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Schneider Electric Security Notification

		<ul style="list-style-type: none"> Ensure that the device is not accessible via the Modbus protocol outside the local network segment by applying appropriate firewalls configuration and controls, and that access to the network segment is protected and controlled.
--	--	--

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>

LEGAL DISCLAIMER

Schneider Electric Security Notification

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’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 14 January 2025	Original Release
---	------------------