Schneider Electric Security Notification

PowerLogic ION7400 / PM8000 / ION9000 Power Meters

9 May 2023 (13 June 2023)

Overview

Schneider Electric is aware of the use of an unsecure protocol in its PowerLogic ION9000, PowerLogic ION7400, PowerLogic PM8000, PowerLogic ION8650, PowerLogic ION8800 and all legacy ION products.

The PowerLogic ION9000, PowerLogic ION7400, PowerLogic PM8000, PowerLogic ION8650 and PowerLogic ION8800 are energy and power quality meters.

The ION Protocol was created over 30 years ago to bring sophisticated data exchange to digital power meters. As cybersecurity became a concern, the protocol was enhanced with support for authentication. More recently, end-to-end encryption support for data in transit using industry standard TLS was released after a multi-year effort to design a solution that would not break backward compatibility with decades of products installed in the field.

This disclosure announces the new secure ION protocol feature for the PowerLogic ION9000, ION7400 and PM8000 products. Secure ION enhances the security of the ION protocol by using a Transport Layer Security (TLS) encrypted tunnel between the device and other systems or software.

June 2023 Update: Additional context has been added to the overview section.

Affected Products and Versions

Product	Version
PowerLogic ION9000, PowerLogic ION7400, PowerLogic PM8000	Prior to 4.0.0
PowerLogic ION8650	All Versions
PowerLogic ION8800	All Versions
Legacy ION products	All Versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2022-46680**

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

A *CWE-319: Cleartext transmission of sensitive information* vulnerability exists that could cause disclosure of sensitive information, denial of service, or modification of data if an attacker is able to intercept network traffic.

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

Affected Product & Version	Remediation
PowerLogic ION9000 *Versions prior to 4.0.0*	Version 4.0.0 and newer of the PowerLogic ION9000 firmware includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/64241-powerlogic-ion9000/#software-and-firmware Additional configuration steps and supporting software are required to utilize the secure ION feature. Please refer to the relevant product documentation or contact customer care for additional details and support.
PowerLogic ION7400 *Versions prior to 4.0.0*	Version 4.0.0 and newer of the PowerLogic ION7400 firmware includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/63502-powerlogic-ion7400/#software-and-firmware Additional configuration steps and supporting software are required to utilize the secure ION feature. Please refer to the relevant product documentation or contact customer care for additional details and support.

PowerLogic PM8000 *Versions prior to v4.0.0*	Version 4.0.0 and newer of the PowerLogic PM8000 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/62252-powerlogic-pm8000-series/#software-and-firmware Additional configuration steps and supporting software are required to utilize the secure ION feature. Please refer to the relevant product documentation or contact customer care for additional details and support.

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.

Mitigations

Affected Product & Version	Mitigations
PowerLogic ION8650 **PowerLogic ION8800** **Legacy ION products**	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Ensure devices that support ION protocol are not exposed to the Internet or other untrusted networks. Apply the best practices for network hardening documented in product user guide and the Schneider Electric Recommended Cybersecurity Best Practices • To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2022-46680	Jos Wetzels, Forescout Technologies

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

Schneider Electric Security Notification

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 empower 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 your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *09 May 2023*	Original Release
Version 1.1 *13 June 2023*	Additional context has been added to the overview section.

Product Security Office Digitally signed by Product Security Office
Date: 2023.06.13 16:07:40 -04'00'