Schneider Electric Security Notification

PowerLogic Power Metering Products

9 February 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM8000 products.

The PowerLogic metering products are revenue and power quality meters for utility and industrial electrical network monitoring.

Failure to apply the mitigations/remediations provided below may risk disclosure of user credentials when using HTTP or Telnet protocol or cause a user to perform an unintended action on a target device when using HTTP, which could result in unintended device behavior.

Affected Products and Versions

Product	Version
ION7400	All versions prior to V3.0.0
ION7650	All versions
ION7700/73xx	All versions. *Note: Only affected by CVE-2021-22702 as these products do not support HTTP web functionality.*
ION83xx/84xx/85xx/8600	All versions.
ION8650	V 4.31.2 and prior.
ION8800	All versions
ION9000	All versions prior to V3.0.0
PM8000	All versions prior to V3.0.0

Vulnerability Details

CVE ID: **CVE-2021-22701**

CVSS v3.0 Base Score 6.2 | Medium | CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:H

A CWE-352: Cross-Site Request Forgery vulnerability exists that could cause a user to perform an unintended action on the target device when using the HTTP web interface.

Schneider Electric Security Notification

CVE ID: **CVE-2021-22702**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-319: Cleartext transmission of sensitive information vulnerability exists that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.

CVE ID: **CVE-2021-22703**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-319: Cleartext transmission of sensitive information vulnerability exists that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.

Remediations

Affected Product & Version	Remediation
ION7400 All versions prior to V3.0.0	V3.0.0 of the PowerLogic ION7400 firmware includes fixes for these vulnerabilities by replacing Telnet functionality with SSH. Additionally, HTTP web interface was removed (only HTTPS mode now supported). The version update files are available for download here: https://www.se.com/ww/en/download/document/ION7400_meter_FW_v003.000.000/ *Note: There may be newer versions of the firmware available for download, please check the ION7400 product page on se.com before upgrading.* Customers who do not wish to apply this remediation should refer to the mitigations below.
ION8650 V4.31.2 and prior	V4.40.1 of the PowerLogic ION8650 firmware includes fixes for these vulnerabilities by replacing Telnet functionality with SSH and making web pages read only. The version update files are available for download here: https://www.se.com/ww/en/download/document/ION8650_meter_FW_V004.040.001/ *Note: There may be newer versions of the firmware available for download, please check the ION8650 product page on se.com before upgrading.* Customers who do not wish to apply this remediation should refer to the mitigations below.

ION9000 All versions prior to V3.0.0	V3.0.0 of the PowerLogic ION9000 firmware includes fixes for these vulnerabilities by replacing telnet functionality with SSH. Additionally, HTTP web interface was removed (only HTTPS mode now supported). The version update files are available for download here: https://www.se.com/ww/en/download/document/ION9000_meter_FW_v003.000.000/ *Note: There may be newer versions of the firmware available for download, please check the ION9000 product page on se.com before upgrading.* Customers who do not wish to apply this remediation should refer to the mitigations below.
PM8000 All versions prior to V3.0.0	V3.0.0 of the PowerLogic PM8000 firmware includes fixes for these vulnerabilities by replacing telnet functionality with SSH. Additionally, HTTP web interface was removed (only HTTPS mode now supported). The version update files are available for download here: https://www.se.com/ww/en/download/document/PM8000_meter_FW_v003.000.000/ *Note: There may be newer versions of the firmware available for download, please check the ION8000 product page on se.com before upgrading.* Customers who do not wish to apply this remediation should refer to the mitigations below.
ION7650	A remediation does not exist for these products, please refer to the Mitigations section below for information on how to reduce the risk of exploit.
ION7700/73xx	
ION83xx/84xx/85xx/8600	
ION8800	

Customers should use appropriate methodologies when applying these upgrades to their devices. We strongly recommend evaluating the impact of these updates in a test and development environment prior to deployment. Contact Schneider Electric's Customer Care Center if you need assistance reverting to an older version of firmware.

Schneider Electric Security Notification

Mitigations

Please refer to your specific products user guide for information on disabling these product features.

Affected Product & Version	Mitigations
ION9000 prior to V3.0.0 ION7400 v2.1.0 to V2.2.1 inclusive PM8000 V2.1.0 to V2.2.1 inclusive	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Disable Telnet functionality • To mitigate plain text HTTP, ensure HTTPS is enabled • To mitigate Cross-Site request forgery, disable HTTP and HTTPS web functionality
ION7400 prior to V2.1.0 PM8000 prior to V2.1.0	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Disable Telnet functionality • Disable HTTP functionality
ION8650 V4.20.1 to 4.31.2 inclusive ION7650 V415 or later ION8800 V362 or later	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Disable Telnet functionality • Disable HTTP web functionality
ION8650 prior to V4.20.1 ION7650 prior to V415 ION8800 prior to V362	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Disable HTTP web functionality A mitigation does not exist for Telnet access. Please upgrade to a newer firmware version and apply the appropriate mitigation.
ION83xx/84xx/85xx/8600 all versions	These products are no longer within a support period. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Disable HTTP web functionality A mitigation does not exist for Telnet access. Customers should also consider upgrading to the latest product offering PowerLogic ION8650 to resolve these vulnerabilities.

ION7700/73xx	These products are no longer within a support period. A mitigation does not exist for Telnet access. Customers should consider upgrading to the latest product offering PowerLogic ION9000, PowerLogic PM8000, or PowerLogic ION7400 to resolve these vulnerabilities.

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 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 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. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *9 February 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.02.07 19:53:54 -05'00'