Schneider Electric Security Notification

PowerLogic ION8650 / ION8800 / ION7x50 / ION7700/73xx / ION83xx/84xx/85xx/8600 Power Meters (V2.0)

9 March 2021 (15 March 2021)

Overview

Schneider Electric is aware of a vulnerability in its PowerLogic ION8650, ION8800, ION7x50, ION7700/73xx, and ION83xx/84xx/85xx/8600 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 meter reboot, which could result in unintended device behavior.

March 2021 update: Affected product reference 'ION7650' changed to 'ION7x50' to encompass all affected product model references in this model series

Affected Products and Versions

Product	Version
ION8650	All versions prior to V4.40.1
ION8800	All versions prior to V372
ION7x50 (Hardware rev. 4 or earlier*)	All versions prior to V376
ION7x50 (Hardware rev. 5*)	All versions prior to V416
ION7700/73xx	All versions
ION83xx/84xx/85xx/8600	All versions

*For details regarding how to determine hardware version, please refer to: https://www.se.com/ww/en/faqs/FA328667/

Vulnerability Details

CVE ID: **CVE-2021-22713**

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

A CWE-119: Improper restriction of operations within the bounds of a memory buffer vulnerability exists that could cause the meter to reboot.

Remediation

Affected Product & Version	Remediation
ION8650 All versions prior to V4.40.1	V4.40.1 (released 4 January 2021) of the PowerLogic ION8650 firmware includes a fix for this vulnerability. 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 before upgrading.*
ION8800	V372 (released 3 March 2021) of the PowerLogic ION8800 firmware includes a fix for this vulnerability. The version update files are available for download here: https://www.se.com/us/en/download/document/ION8800_V372/ *Note: There may be newer versions of the firmware available for download, please check the ION8800 product page before upgrading.*
ION7x50 (Hardware rev. 4 or below)	V376 (released 3 March 2021) of the PowerLogic ION7x50 firmware includes a fix for this vulnerability. The version update files are available for download here: https://www.se.com/us/en/download/document/ION7x50_v376/ *Note: There may be newer versions of the firmware available for download, please check the ION7x50 product page before upgrading.*
ION7x50 (Hardware rev. 5)	V416 (released 3 March 2021) of the PowerLogic ION7x50 firmware includes a fix for this vulnerability. The version update files are available for download here: https://www.se.com/us/en/download/document/ION7x50_V416/ *Note: There may be newer versions of the firmware available for download, please check the ION7x50 product page before upgrading.*

ION7700/73xx	These products are no longer within a support period. Customers should consider upgrading to the latest product offering PowerLogic ION9000, PowerLogic PM8000, or PowerLogic ION7400 to resolve this issue. Contact your local authorized sales representative or Schneider Electric country office for additional guidance.
ION83xx/84xx/85xx/8600	These products are no longer within a support period. Customers should consider upgrading to the latest product offering PowerLogic ION8650 to resolve this issue. Contact your local authorized sales representative or Schneider Electric country office for additional guidance.

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.

For alternative mitigations, customers should follow the General Security Recommendations provided below to reduce the risk of exploit.

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.

Schneider Electric Security Notification

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

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

CVE	Researchers
CVE-2021-22713	Tal Keren and Rei Henigman of Claroty

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

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 March 2021*	Original Release
Version 2.0 *15 March 2021*	Updated affected product reference 'ION7650' to 'ION7x50' to encompass all affected product model references in this model series (page 1-2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.03.15 10:01:45 -04'00'