

Schneider Inverter and Schneider Boost

Security Handbook

Schneider Inverter: HY8K3EU1, HY10K3EU1, HY14K3EU1, HY5K1EU1, HY6K1EU1, and HY8K1EU1

Schneider Boost: BAT7KEU1, BAT10KEU1, BAT14KEU1, BAT17KEU1, and BAT20KEU1

October 2024

Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

See the latest version of this guide at: <https://www.se.com/>

Contact Information

For country-specific details, please contact your local Schneider Electric Sales Representative or visit the Schneider Electric website at: <https://www.se.com/>

Validity Note

This document is valid only for the Schneider Inverter HY8K3EU1, HY10K3EU1, HY14K3EU1, HY5K1EU1, HY6K1EU1, and HY8K1EU1, and Schneider Boost BAT7KEU1, BAT10KEU1, BAT14KEU1, BAT17KEU1, and BAT20KEU1.

If this manual is in any language other than English, although steps have been taken to maintain the accuracy of the translation, the accuracy cannot be guaranteed. Approved content is contained with the English language version which is posted at <https://www.se.com/>.

The characteristics of the products described in this document are intended to match the characteristics that are available on <https://www.se.com/>. As a part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on <https://www.se.com/>, consider <https://www.se.com/> to contain the latest information.

Contents

Legal Information	2
Contact Information	2
Validity Note	3
Cybersecurity in Schneider Electric	8
Introduction	8
Cybersecurity Policies	8
Cybersecurity Resources	8
Security Capabilities and Recommendations	12
Supported Protocols	13
Potential Risks and Compensating Controls	13
Security Recommendations	14
Decommissioning	16
Dispose of Physical Device	16

1 Cybersecurity in Schneider Electric

What's in This Chapter?

Cybersecurity in Schneider Electric	8
Introduction	8
Cybersecurity Policies	8
Cybersecurity Resources	8

Cybersecurity in Schneider Electric

Introduction

Cybersecurity is integral to Schneider Electric's business strategy and follows a cybersecurity posture that covers many aspects, such as:

- Helping to secure internal activities.
- Providing elevated levels of protection of strategic IT systems and assets.
- Leading the digital transformation within a cybersecure framework.
- Designing and developing new products and solutions with end-to-end cybersecure measures and protection.

Cybersecurity Policies

To support the development and maintenance of secure products, Schneider Electric follows a Secure Development Lifecycle (SDL) compliant with the IEC 62443-4-1 Security Standard for Industrial Automation and Control systems.

It consists of implementing a process that relies on security best practices and dedicated tools that cover:

- Security training for teams involved in the product design, development, and testing.
- Threat modeling analysis and security design reviews.
- Static code analysis and code security reviews.
- Periodic penetration and vulnerability testing.
- Stringent vulnerability management process.

Cybersecurity Resources

Cybersecurity Solutions

For recommendations and guidance on how to help secure the environment and infrastructure in which the Prosumer Storage System (Schneider Inverter and Schneider Boost) is deployed, Schneider Electric publishes guidelines, white papers, and best practices that can be consulted at <https://www.se.com/>.

Cybersecurity Support Portal

Other cybersecurity resources can be found at the [Schneider Electric Cybersecurity Support Portal](#), including:

- Schneider Electric's vulnerability management policy.
- Security Notifications about vulnerabilities in products and systems.

Schneider Electric's vulnerability management policy addresses cybersecurity vulnerabilities affecting Schneider Electric products in order to help support the security and safety of our customers.

Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to help ensure that accurate information is provided in a timely fashion in order to better protect customer installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and alerting customers about vulnerabilities and mitigations affecting products.

The [Schneider Electric Cybersecurity Support Portal](#) also provides interfaces to report cybersecurity vulnerabilities and to register to the Security Notification updates mailing list to keep customers informed via email on newly released or updated Security Notifications.

2 Security Capabilities and Recommendations

What's in This Chapter?

Security Capabilities and Recommendations	12
Supported Protocols	13
Potential Risks and Compensating Controls	13
Security Recommendations	14

Security Capabilities and Recommendations

Security Features

Security features have been built into the Prosumer Storage System (Schneider Inverter and Schneider Boost) to help ensure that the product operates as intended.

These features provide more security capabilities which are expected to better protect the product from potential security threats that could disrupt the product operation (availability), modify the product configuration (integrity), or disclose information (confidentiality).

The key features are:

- Firmware update mechanism with firmware signature verification (using asymmetric cryptography)
- TLS 1.2 for securing and authenticating MQTT S communications with a remote management system (ETP)
- Common Criteria EAL6+ certified security chip for storing the product authenticity key and certificate
- Protection of sensitive data stored in the Wireless LAN Smart Dongle using robust cryptography (AES-256)
- Deactivation of internal debug and test interfaces

These security capability features aim to mitigate the threats related to the usage of the Prosumer Storage System (Schneider Inverter and Schneider Boost) in its intended environment (User Home).

The effectiveness of these capabilities depends on the adoption and application of the recommendations provided in this guide to cover the commissioning, operation, maintenance, and decommissioning of the Prosumer Storage System (Schneider Inverter and Schneider Boost), as well as [recommended cybersecurity best practices](#).

Supported Protocols

The following protocols are supported by the Prosumer Storage System (Schneider Inverter and Schneider Boost):

Table 1 Supported protocols

Protocol	Usage
MQTT (TLS 1.2)	TLS 1.2 for securing and authenticating MQTT communications with a remote management system (ETP)
BLE X.X (with encryption)	Configuration through eSetup/Wiser Home app
Modbus RTU	Communications with Modbus Slave
CAN	Communications inside the battery
Wi-Fi	Communications with Home Router

Potential Risks and Compensating Controls

Table 2 Potential risks and compensating controls

Area	Issue	Risk	Compensating Controls
Physical access	A Prosumer Storage System (Schneider Inverter and Schneider Boost) may be subject to tampering attempts	If the Prosumer Storage System (Schneider Inverter and Schneider Boost) is accessed by a malicious user and its content is altered, malfunctions or possible damages may occur.	Periodically inspect the Schneider Inverter and Schneider Boost for evidence of tampering attempts (scratches, tears, rips, etc.). Install the Schneider Inverter and Schneider Boost in a controlled environment or install security cameras.
Communication protocols	Modbus RTU, CAN are unsecure	Modbus RTU and CAN are used for internal communication of Prosumer Storage System (Schneider Inverter and Schneider Boost). If a malicious user has gained access to the network, it is possible to intercept and eavesdrop communications.	Periodically inspect the Schneider Inverter and Schneider Boost for evidence of tampering attempts (scratches, tears, rips, etc.). Install the Schneider Inverter and Schneider Boost in a controlled environment or install security cameras.

Security Recommendations

Configuration of Services

Most Prosumer Storage System (Schneider Inverter and Schneider Boost) services are disabled by default to reduce the attack surface and exposure to a minimum. Schneider Electric recommends only enabling the services that are strictly required. Unused services should be kept disabled. Similarly, when a service is not needed or used anymore, it is advised to disable it.

Firmware Update

The Prosumer Storage System (Schneider Inverter and Schneider Boost) embeds a digital firmware that may require the application of security patches to maintain an optimum level of security. Schneider Electric recommends periodically verifying that the installed firmware is the latest one available.

In addition, product owners are invited to consult and register to the [Schneider Electric Cybersecurity Support Portal](#) to stay informed on newly released or updated Security Notifications.

Audit Log

The Prosumer Storage System (Schneider Inverter and Schneider Boost) maintains an audit log that tracks security-related events such as reboots and firmware updates.

Schneider Electric recommends consulting the audit log on a regular basis to detect potential unexpected or incorrect behaviors.

3 Decommissioning

What's in This Chapter?

Decommissioning	16
Dispose of Physical Device	16

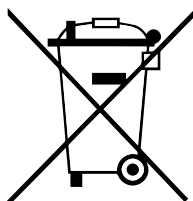
Decommissioning

When decommissioning the Prosumer Storage System (Schneider Inverter and Schneider Boost), you must reset the settings of the product to erase confidential user information and prevent this information from being disclosed or reused.

You must also reset the PIN code and remove the Wi-Fi credentials when decommissioning.

See the latest versions of the Schneider Inverter and Schneider Boost installation guides on <https://www.se.com/> for instructions on how to decommission the Prosumer Storage System (Schneider Inverter and Schneider Boost).

Dispose of Physical Device



Electric appliances marked with the symbol shown must be professionally treated to recover, reuse, and recycle materials in order to reduce negative environmental impact. When the product is no longer usable, the consumer is legally obligated to ensure that it is collected separately under the local electronics recycling and treatment scheme.

Customer Support

Customer support for this or any other product is available at no charge by visiting the Schneider Electric website at <https://www.se.com/> and submitting customer support requests.

For information on how to obtain local customer support, contact the Schneider Electric representative or other distributor from whom you purchased your Schneider Inverter.

Contact Schneider Electric customer service:

- Germany: <https://www.se.com/de/de/work/support/customer-care/contact-schneider-electric.jsp>
- Spain: <https://www.se.com/es/es/work/support/customer-care/contact-schneider-electric.jsp>

Schneider Electric

201 Washington St, Suite 2700, One Boston Place
Boston, Massachusetts 02108
United States
<https://www.se.com/>

As standards, specifications, and designs change from time to time,
please ask for confirmation of the information given in this
publication.

For other country details please contact your local Schneider
Electric Sales Representative or visit the Schneider Electric website
at: <https://www.se.com/>

© 2024 Schneider Electric. All Rights Reserved.