EVlink Pro AC

Cybersecurity Guide

GEX5261101-02
01/2024

www.se.com

Schneider Electric

Legal Information

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained by qualified personnel only. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK
- Do not open the product.
- Product to be serviced by qualified people only.

Failure to follow these instructions will result in death or serious injury.

NOTE: All instructions applicable to the enclosed product and all safety precautions must be observed.

For more information, you can connect with the Customer Care Center by using the following QR code:

About the Book

Document Scope

This guide is intended to provide information about the cybersecurity capabilities and features of the EVlink Pro AC product as well as recommendations to ensure the product is installed, operated, and maintained while retaining its intended level of security during its whole lifecycle.

The content of this document is applicable to EVlink Pro AC products with a firmware version 1.0.2 or higher.

Related Documents

Title of documentation	Reference number
EVlink Pro AC OCPP Connectivity Guide	GEX1969200
EVlink Pro AC Modbus Connectivity Guide	GEX1969300

You can download these technical publications and other technical information from our website at www.se.com/ww/en/download/.

Cybersecurity Information

Notice

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first step to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Important Information

The EVlink Pro AC Charging Station supports to be connected to Ethernet networks, however this networking capability is not designed to withstand the direct exposure to the public Internet.

The EVlink Pro AC Charging Station is intended to be used in a trusted network environment, for instance, behind firewalls, and/or within the boundaries of an isolated OT network (separated from the IT network).

More information can be obtained by consulting Schneider Electric recommended cybersecurity best practices or Cybersecurity Solutions.

Cybersecurity in Schneider Electric

Introduction

Cybersecurity is integral to Schneider Electric's business strategy and it follows a Cybersecurity posture that covers many aspects:

- Securing 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 in implementing a process relying on security best practices, dedicated tools that covers:

- 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 secure the environment and infrastructure in which the EVlink Pro AC Charging Station is deployed, Schneider Electric publishes guidelines, white papers, and best practices that can be consulted in the Cybersecurity Solutions page of Schneider Electric global website.

Cybersecurity Support Portal

In addition, other resources can be found in Schneider Electric Cybersecurity Support Portal, including:

- Schneider Electric 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 support the security and safety of our customers.
Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect customer installations.

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

The Cybersecurity Support Portal also provides interfaces to report cybersecurity vulnerabilities and to register to the security notification updates mailing list to stay informed via email on newly released or updated Security Notifications.

Security Features

Security features have been built into the EVlink Pro AC Charging Station to ensure that the product operates accordingly to its intended purpose.

These features will provide security capabilities which are expected to protect the product from potential security threats that could allow disrupting the product operation (availability), modifying the product configuration (integrity) or disclosing information (confidentiality).

The key features are:

- Firmware authenticity verification at product startup (secure boot),
- Firmware update mechanism (either local via the commissioning app or remote via OCPP) with firmware signature verification (using asymmetric cryptography),
- TLS 1.2 for securing and authenticating OCCP communications with a remote charging station management system (CSMS),
- Common Criteria EAL6+ certified security chip for storing the product authenticity key and certificate,
- Protection of sensitive data stored in the product using robust cryptography (AES-256),
- Export of maintenance reports and configuration in encrypted archives,
- Reset mechanism to erase all user sensitive information stored in the product.

However, the effectiveness of these capabilities will depend on the adoption and application of the recommendations provided in this guide to cover the commissioning, operation, maintenance and decommissioning of the EVlink Pro AC Charging Station, as well as recommended cybersecurity best practices.

Supported Protocols

The following protocols are supported by the EVlink Pro AC Charging Station:

Protocol	Usage
OCPP (TLS 1.2)	Communications with a remote Charging Station Management System (CSMS) Note: The OCPP protocol relies on additional HTTP(S)/FTP(S) communications for supporting OCPP reporting and maintenance operations (firmware update)
Bluetooth Low Energy 4.2	Configuration through eSetup configuration app
HTTPS (TLS 1.2)	Configuration through configuration tools

SSH	Advanced diagnostics Notes: - SSH interface usage is restricted to Schneider Electric support engineering teams - SSH service is disabled by default and can be enabled punctually through eSetup configuration app for expertise needs
Modbus TCP/Modbus-SL	Communications with power meters and/or Building Management Systems (BMS),
DHCP	Networking IP address
DNS	Network name resolution
SSDP	Network discovery
SMTPS (TLS 1.2)	Sending of charge operation reports via email
ISO/IEC 14443A/B ISO/IEC 15693	User authentication with RFID badges

Potential Risks and Compensating Controls

Area	Issue	Risk	Compensating controls
Physical access	A charging station may be subject to tampering attempts	If the charging station is access by a malicious user and its content is altered, malfunctions or possible damages may occur.	Periodically inspect the charging station for evidence of tampering attempts (scratches, tears, rips…). Install the charging station in a controlled environment or install security cameras.
RFID badges	A badge may be forged or duplicated	If a malicious user gets his hands on an RFID badge, he may be able to duplicate it and spoof the identify of a legitimate charging station user.	Do not let RFID badges unattended. In case of suspicion of potential badge duplication or forgery, revoke and renew badges.
Maintenance user account	Default credentials are often the source of unauthorized access by malicious users	If the charging station has not been commissioned and the default PIN code is left unchanged, unauthorized access can occur.	Update the default PIN code using the commissioning app. Also consider renewing the PIN code on a regular basis.
	Same user account PIN codes are used in different charging stations	If the PIN code is known by a malicious user, he could also access to all other charging stations configured with the same PIN code	When installing several charging stations, configure different PIN codes in each charging station

Communication protocols	Modbus TCP, DHCP, DNS and SSDP are unsecure	If a malicious user has gained access to the network, it is possible to intercept and eavesdrop communications	For transmitting data over an internal network, physically or logically segment the network For transmitting data over an external network, consider encapsulating communications in an encrypted tunnel, a TLS wrapper or a similar solution.
USB port	A USB key or USB storage device may contain a malware	If a malware such as viruses, Trojans, worms is present in the USB key or USB storage device, it might spread to the Charging Station and malfunctions, data deletion or information disclosure may occur.	Analyze the USB key or USB storage device content with an anti-virus software before plugging it into the Charging Station USB port
Bluetooth connectivity	When Bluetooth interface is available, the charging station becomes remotely accessible over-the-air	A malicious user located nearby the charging station may try to connect and to attempt to abuse it while the Bluetooth interface is available.	Limit the Bluetooth exposure by ensuring the charging station has been commissioned and that an administration badge has been configured (refer to recommendations for commissioning section below).

Security recommendations

Recommendations for Commissioning

Default PIN code

A default user account is provisioned in the EVlink Pro AC Charging Station for supporting the initial connection to the product with commission app during the installation.

The PIN code for this account is described in the user documentation. It is thus recommended to replace it with a new PIN code using the commissioning app.

The new PIN code should follow security best practices such as using a minimum of 6 digits and avoiding easily guessable patterns (blocks of similar digits or sequential increments of digits).

OCPP communication security

When configuring the EVlink Charging Station to connect to a remote Charging Station Management System with OCPP, it is recommended to always use WSS or HTTPS to secure the communication.

Communications relying on plain HTTP or plain Web Sockets are unsecure and are subject to Man-In-The-Middle attacks.

Configuration of Services

Most EVlink Pro AC Charging Station services are disabled by default to reduce the attack surface and exposure to a minimum.
Consequently, it is recommended to only enable 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.

Bluetooth security

By default, the Bluetooth interface is automatically enabled for a 2-hour period immediately after the charging station has started, in order to provide a time window allowing to perform the commissioning operations.

To secure the Bluetooth interface and reduce its exposure to a minimum, it is recommended to configure an administration badge. This will have the effect to deactivate the automatic Bluetooth activation at startup and to replace it by an activation mechanism controlled by the badge.

For convenience purpose (but at the expense of lesser security) it remains possible through the advanced settings of eSetup configuration app to re-enable the automatic Bluetooth activation at startup.

Security Recommendations for Maintenance

Firmware update

The EVlink Pro AC Charging Station is embedding a digital firmware that may require the application of security patches to maintain an optimum level of security.
Consequently, it is recommended to periodically verify that the installed firmware is the latest one available.

Firmware updates and release notes can be downloaded from our website at EVlink Pro AC | Schneider Electric Global (se.com).
In addition, product owners are invited to consult and register to Schneider Electric cybersecurity portal to stay informed on newly released or updated Security Notifications.

Audit Log

The EVlink Pro AC Charging Station maintains an audit log tracking security related events such as reboot, firmware update, invalid login attempts…

It is recommended to consult the audit log on a regular basis to detect potential unexpected or incorrect behaviors.

Security Recommendations for Decommissioning

Reset to factory settings

The EVlink Pro AC Charging Station can process confidential user information, which may include user account identifiers and passwords, RFID badge identifiers as well as charge operations history.

When disposing, recycling or before a change of ownership of the product, it is required to perform a reset to factory settings of the product to erase all personal data and sensible or confidential user information and ensure it cannot be disclosed or reused.

Removal of personal data

Personal data stored or cached in the product can be deleted through a reset to factory settings operation (procedure details are documented in the Installation Guide available in the EVlink Pro AC documentation page (se.com).

In addition, if the product is connected to a supervision system, please contact your charging point operator to request the removal of personal data that are stored by the supervision system and associated services.

If the reset to factory settings operation cannot be performed (for instance due to a faulty EVlink Pro AC charging station), please contact Schneider Electric support.

Glossary

AC	Alternative Current
BMS	Building Management System
CERT	Cyber Emergency Response Team
CSMS	Charging Station Management System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level
EV	Electric Vehicle
FTP/FTPS	File Transfer Protocol / File Transfer Protocol Secure
HTTP/HTTPS	Hyper-Text Transfer Protocol / Hyper-Text Transfer Protocol Secure
IEC	International Electrotechnical Commission
IT	Information Technology
OCPP	Open Charge Point Protocol
OT	Operational Technology
PIN	Personal Identification Number
RFC	Request For Comments
RFID	Radio Frequency Identification
SDL	Secure Development Lifecycle
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
WS/WSS	WebSocket / WebSocket Secure

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison – France
+ 33 (0) 1 41 29 70 00
www.se.com

GEX5261101-02