Cybersecurity Guide

Cybersecurity Information

Important information

EVlink Home Smart charging stations support to be connected to Ethernet/Wi-Fi networks, however this networking capability is not designed to withstand the direct exposure to the public Internet.

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use 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.

Cybersecurity at 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 Cybersecurity measures and protection.

Cybersecurity Policies

To support the development and maintenance of 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 help securing the environment and infrastructure in which EVlink Home Smart charging stations are 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 help improving the security of our customers.
Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to help ensuring that accurate information is provided in a timely fashion to help protecting 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 EVlink Home Smart charging stations to help ensuring that products operate accordingly to the intended purpose.

These features will provide security capabilities which are expected to protect the products 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 (local via the commissioning app and remote via OCPP) with firmware signature verification (using asymmetric cryptography),
- TLS 1.2 to help securing and authenticating OCCP communications with a remote charging station management system (CSMS),
- Deactivation of internal debug and test interfaces.

These security capability features are aiming at mitigating the threats related to the usage of the EVlink Home Smart charging stations in their intended environments.

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 of EVlink Home Smart charging stations, as well as recommended cybersecurity best practices.

Supported Protocols

The following protocols are supported by EVlink Home Smart charging stations:

Protocol	Usage
OCPP (TLS 1.2) + HTTPS/SFTP	Communications with a remote Charging Station Management System (CSMS) Note: The OCPP protocol relies additional HTTPS/FTPS communications for supporting OCPP reporting and maintenance operations (firmware update)
HTTPS (TLS 1.2)	Configuration through configuration tools

Modbus RTU	Communications with power meters
DHCP	Networking IP address
DNS	Network name resolution

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 accessed 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.
Maintenance user account	Default credentials are often the source of unauthorized access by malicious users	If the charging station has not been commissioned and no customized PIN is defined by the user, unauthorized access can occur.	Defined a customized PIN code using the commissioning app. Also consider renewing the PIN code on a regular basis.
Communication protocols	Modbus RTU, DHCP, DNS are unsecure	If a malicious user has gained access to the network, it is possible to intercept and eavesdrop communications	For transmitting data over a residential network, consider applying WPA authentication with a robust password for Wi-Fi network or activating secured pairing functionality for Power Line Communication (PLC) network

Security recommendations

Recommendations for Commissioning

Default PIN code

The user is forced to define a customized PIN code at first connection of the commissioning app to EVlink Home Smart charging stations.

The 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).

Configuration of Services

Most EVlink Home Smart 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.

Security Recommendations for Maintenance

Firmware update

EVlink Home Smart charging stations are embedding a digital firmware that may require application of security patches to maintain an optimum level of security.
Consequently, it is recommended to periodically check that the installed firmware is the latest one available.

Firmware updates and release notes can be downloaded from our eSetup for electrician application