EcoStruxure™ EV Charging Expert

Cybersecurity Guide

DOCA0349EN-01
03/2024

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 EV Charging Expert product as well as recommendations to help ensure the product is installed, operated, and maintained to preserve a secure operating environment for the product.

This document does not address in-depth the aspects to help protect an operational technology network but provides guidance and security best practices to that aim.

The content of this document is applicable to EV Charging Expert products with a firmware version 5.2 or higher.

Related Documents

Title of documentation	Reference number
EcoStruxure™ EV Charging Expert User Guide	DOCA0163EN
EcoStruxure™ EV Charging Expert Install Guide	DOCA0164EN

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 EV Charging Expert supports to be connected to Ethernet networks, however this networking capability is not designed to withstand the direct exposure to the public Internet or external unsecure networks.

The EV Charging Expert 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 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.

Cybersecurity Resources

Cybersecurity Solutions

For recommendations and guidance on how to help secure the environment and infrastructure in which the EV Charging Expert 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 help support the security 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 to help 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.

Environment and network security

The EV Charging Expert is designed to be used in a protected environment and deployed following a defense-in-depth strategy.

Defense-in-depth

Defense in depth is a multi-layered approach that leverages and combines several cybersecurity measures and controls helping to increase the device environment protection by reducing the attack surface.

Before you install the EV Charging Expert, review the following guidance. If you have not already adopted these best practices, we strongly advise to implement these recommendations to help improve your cybersecurity posture and to reduce the exposure to potential vulnerabilities.

Environment security

Site security

EV Charging Expert is intended to be installed in an access controlled or monitored location environment.

Physical security

Physical controls or protections should be deployed to restrict the physical access to the EV Charging Expert to authorized persons only. This encompasses measures such as keeping the product in locked switchboards or cabinets.

Network security

Network segregation and segmentation

The EV Charging Expert is not designed to withstand direct exposure to the public Internet or external networks beyond the boundaries of the EV infrastructure local area network.

It is recommended to deploy EV Charging Expert and EV charging stations in a local area network (LAN) dedicated to the EV charging infrastructure digital communications, separated from other networks.

In case of interconnection needs between the EV charging networks and other networks, it is required to separate the EV charging infrastructure LAN by creating Demilitarized Zones (DMZ) to isolate and help protect other networks by using technologies such as network firewalls, network access control, data diodes.

In addition, physically and logically segmenting the network using routers and Virtual Local Area Networks (VLAN) should be considered.

Network monitoring

Continuous monitoring for events that might indicate attempted unauthorized access to the network or devices is recommended to minimize the chances of a compromise.

Equipment such as Intrusion detection systems (IDS) and intrusion prevention systems (IPS) help detect and prevent suspicious or malicious activities.

Embedded web server

The EV Charging Expert is equipped in factory with a default x.509v3 certificate allowing to enable HTTPS communications when accessing its embedded web server.

This certificate is not issued by a Certificate Authority for the public Internet and consequently web browsers display a security warning when trying to connect to the EV Charging Expert web pages.

To help ensure the connection is secure, it is recommended to use a direct Ethernet connection between the EV Charging Expert and the computer used to access the web server.

Product cybersecurity capabilities

Security Features

Security features have been built into the EV Charging Expert to help ensure that the product operates accordingly to the intended purpose.

These features will provide security capabilities which are expected to help 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:

- Authentication and authorization controls of user access when connecting to the embedded web pages,
- OCPP secure communications (supporting integrity, confidentiality and authenticity) with TLS 1.2 between the EV Charging Expert and a remote CSMS,
- OCPP secure communications with TLS 1.2 (supporting integrity and confidentiality) between the EV Charging Expert and connected EV charging stations,
- HTTP secure communications (supporting confidentiality and integrity) with TLS 1.2 when accessing to the product from the web pages,
- Application firmware update mechanism,
- Protection of stored user accounts password using approved cryptography (hash and salt),
- Back to factory settings reset mechanism to wipe user data to support product secure disposal,

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 EV Charging Expert, as well as recommended cybersecurity best practices.

Supported Protocols

The following protocols are supported by the EV Charging Expert:

Protocol	Usage
OCPP (TLS 1.2)	Communications with both EV charging stations and 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)
HTTPS (TLS 1.2)	Configuration through embedded web pages Web services for remote commissioning of Schneider Electric charging stations Web services for connectivity with external Energy Management System (EMS)
SSH	Advanced diagnostics Notes: - SSH interface usage is restricted to Schneider Electric support engineering teams - SSH service is disabled in factory settings - SSH service can be enabled for advanced auditing or troubleshooting by the product owner through the embedded web pages settings upon Schneider Electric request
Modbus TCP Modbus RTU	Communications with power meters and/or Building Management Systems (BMS),
DHCP	Networking IP address
DNS	Network name resolution
SSDP	Network discovery

Potential Risks and Compensating Controls

Area	Issue	Risk	Compensating controls
Physical access	EV Charging Expert may be subject to tampering attempts	If the EV Charging Expert is access by a malicious user and its integrity is compromised, malfunctions or possible damages may occur.	Install the EV Charging Expert in a controlled environment (locked switchboard or room) or install security cameras. Periodically inspect the EV Charging Expert for evidence of tampering attempts (scratches, tears, rips…).
Maintenance user accounts	Same user account passwords are used in different EV Charging Expert	If a shared user account password is known by a malicious user, he could also access to all other EV Charging Expert configured with the same password	When installing several EV Charging Expert, configure different user account passwords 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.
Embedded web server	The server is equipped with a self-signed certificate	If a malicious user has access to the network, it is possible to impersonate the EV Charging Expert web server and gain access to user information	It is recommended to use a direct Ethernet connection between the EV Charging Expert and the computer use to access the web server
SD card reader	The SD card reader may be subject to abuse or hack attempts	If a malicious user has access to the SD card reader, it may be able to perform arbitrary code execution or steal data.	Restrict the reader access by installing an SD port blocker In addition, ensure Physical Access compensating controls are deployed
USB and HDMI ports	The media ports may be subject to abuse or hack attempts	If a malicious user can connect a keyboard and/or a display to the media ports, he may be able to gather information and/or to attempt to obtain a local console access	Restrict the ports access by installing USB and HDMI port blockers. In addition, ensure Physical Access compensating controls are deployed
EV charging stations	Rogue devices may attempt to impersonate EV charging stations	If a malicious user has access to the network, it is possible to impersonate an EV charging station and hijack or tamper OCPP communications with the EV Charging Expert	Monitor the network for potential incoming OCCP connection attempts using the same box identifiers and originating from different IP addresses Review periodically the EV Charging Expert settings and verify that no unexpected device has been enrolled in the configuration.

Product security recommendations

Recommendations for Commissioning

Enrollment of EV charging stations

The EV Charging Expert features a discovery mechanism to simply the enrollment of new EV charging stations in its configuration.

During the enrollment process, verify the list of discovered EV charging stations before adding them to the configuration and help ensure that no unexpected device is enrolled in the EV Charging Expert configuration.

OCPP communication security

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

Communications relying on plain OCCP with plain Web Sockets and HTTP are unsecure and may be subject to Man-In-The-Middle attacks.

Security Recommendations for Maintenance

Firmware application update

The EV Charging Expert is running an application 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.

Application firmware updates and release notes can be downloaded from our website at https://www.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.

Charging stations management

The EV infrastructure may evolve over time, as new EV charging station can be added, replaced or alternatively older EV charging stations can be removed and decommissioned.

In the latter case, verify that when an EV charging station is removed from the infrastructure, the EV Charging Expert settings are updated to reflect the change by removing the station identifier from the configuration.

Audit Log

The EV Charging Expert 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 unexpected or incorrect behaviors that could indicate potential product abuse attempts.

Security Recommendations for Decommissioning

Reset to factory settings

The EV Charging Expert can process confidential user information, which may include user account identifiers and passwords, RFID badge identifiers as well as the history of charge transactions.

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 help 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.

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, 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
EMS	Energy Management System
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
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