Schneider Electric Security Notification

EVlink City / Parking / Smart Wallbox Charging Stations

13 July 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its EVlink City, Parking and Smart Wallbox products.

The EVlink products are electric vehicle (EV) charging stations for home, private properties, semi-public car parks and on-street charging.

These vulnerabilities can be exploited by obtaining physical access either to the charging station's internal communication port, which requires disassembling the charging station enclosure, or, in the case of a connected station, to the network of the charging station's supervision system. The risk is further elevated when the connected stations are accessible over the internet and have insufficient network security measures.

Customers should immediately apply the available remediations, failure to do so may risk potential unauthorized access to the charging station's web server, which could lead to tampering and comprise of the charging station's settings and accounts. Such tampering could lead to things like denial of service attacks, which could result in unauthorized use of the charging station, service interruptions, failure to send charging data records to the supervision system and the modification and disclosure of the charging station's configuration.

In addition to applying the available remediations, to limit the risk of a connected charging station being compromised, Schneider Electric recommends that customers follow and apply network security best practices and ensure that the charging stations are not accessible from the internet, as outlined in the General Security Recommendations section.

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Affected Products and Versions

Product	Version
EVlink City EVC1S22P4 / EVC1S7P4	All versions prior to R8 V3.4.0.1
EVlink Parking EVW2 / EVF2 / EV.2	All versions prior to R8 V3.4.0.1
EVlink Smart Wallbox EVB1A	All versions prior to R8 V3.4.0.1

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2021-22706**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.

CVE ID: **CVE-2021-22707**

CVSS v3.1 Base Score 9.4 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists that could allow an attacker to issue unauthorized commands to the charging station web server with administrative privileges.

CVE ID: **CVE-2021-22708**

CVSS v3.1 Base Score 7.2 | High | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists that could allow an attacker to craft a malicious firmware package and bypass the signature verification mechanism.

CVE ID: **CVE-2021-22721**

CVSS v3.1 Base Score 5.8 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

A *CWE-200: Information Exposure* vulnerability exists that could allow an attacker to get limited knowledge of javascript code when crafted malicious parameters are submitted to the charging station web server.

CVE ID: **CVE-2021-22722**

CVSS v3.1 Base Score 8.9 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:L

A C*WE-79: Improper Neutralization of Input During Web Page Generation ('Stored Cross-site Scripting') v*ulnerability exists that could cause code injection when importing a CSV file or changing station parameters.

CVE ID: **CVE-2021-22723**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') through Cross-Site Request Forgery (CSRF)* vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.

CVE ID: **CVE-2021-22726**

CVSS v3.1 Base Score 8.2 | High | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L

A *CWE-918: Server-Side Request Forgery (SSRF)* vulnerability exists that could allow an attacker to perform unintended actions or access to data when crafted malicious parameters are submitted to the charging station web server.

CVE ID: **CVE-2021-22727**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

A *CWE-331: Insufficient Entropy* vulnerability exists that could allow an attacker to gain unauthorized access to the charging station web server.

CVE ID: **CVE-2021-22728**

CVSS v3.1 Base Score 7.7 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

A *CWE-200: Information Exposure* vulnerability exists that could cause disclosure of encrypted credentials when consulting the maintenance report.

CVE ID: **CVE-2021-22729**

CVSS v3.1 Base Score 9.4 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

A *CWE-259: Use of Hard-coded Password* vulnerability exist that could allow an attacker to gain unauthorized administrative privileges when accessing to the charging station web server.

CVE ID: **CVE-2021-22730**

CVSS v3.1 Base Score 9.4 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists that could an attacker to gain unauthorized administrative privileges when accessing to the charging station web server.

CVE ID: **CVE-2021-22773**

CVSS v3.1 Base Score 6.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

A *CWE-620: Unverified Password Change* vulnerability exists that could allow an attacker connected to the charging station web server to modify the password of a user.

CVE ID: **CVE-2021-22774**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

A *CWE-759: Use of a One-Way Hash without a Salt* vulnerability exists that could lead an attacker to get knowledge of charging station user account credentials using dictionary attacks techniques.

Remediation

Version R8 V3.4.0.1 of the EVlink City, Parking and Smart Wallbox products include a fix for these vulnerabilities and is available by contacting Schneider Electric's Customer Care Center or for download below:

Product & Version	Version
EVlink City EVC1S22P4 / EVC1S7P4	https://www.se.com/fr/fr/product-range-download/63015-evlink-city/#/software-firmware-tab
EVlink Parking EVW2 / EVF2 / EV.2	https://www.se.com/ww/en/product-range/60850-evlink-parking/#software-and-firmware
EVlink Smart Wallbox EVB1A	https://www.se.com/ww/en/product-range/63506-evlink-smart-wallbox/#software-and-firmware

To ensure the fix is applied, the new firmware version can be verified by connecting to the station web server and consulting the firmware update tab in the maintenance section. The version for both the electronic board and the commissioning tool is 3400-1 or newer.

Contact Schneider Electric's Customer Care Center if you need assistance applying the patch.

If customers choose not to apply the remediation provided above, they should follow the recommendations provided in the General Security Recommendations section below in order to harden the security of the network where the charging station is connected (in case of a supervised station) and ensure that the station is not reachable from outside the network.

Schneider Electric Security Notification

Recommendations for End of Life Offers

EVlink Parking products with references EVF1 / EVW1 and EVlink City products with references EVC1S22P3 / EVC1S7P3 or older have reached their end of life and are no longer supported.

Customers should consider replacing the charging station by the latest EVlink Parking and EVlink City product offering to resolve these issues. Always follow the recommendations provided in the General Security Recommendations section below in order to harden the security of the network where the charging station is connected (in case of a supervised station) and ensure that the station is not reachable from outside this network.

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.

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 these vulnerabilities:

CVE	Researchers
CVE-2021-22706	• Tony Marcel Nasr • Wu Ming (BaCde) and Chen Huajiang (Kevin2600)
CVE-2021-22707 CVE-2021-22708	• Wu Ming (BaCde) and Chen Huajiang (Kevin2600) • Stefan Viehböck (SEC Consult)
CVE-2021-22721 CVE-2021-22722 CVE-2021-22723 CVE-2021-22726 CVE-2021-22727 CVE-2021-22728	• Tony Marcel Nasr
CVE-2021-22729	• Guillaume Jonville (B2EI) • Tony Marcel Nasr
CVE-2021-22730 CVE-2021-22773 CVE-2021-22774	• Tony Marcel Nasr

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

IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION

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 *13 July 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.07.12 20:26:11 -04'00'