EcoStruxure EV Charging Expert

08 February 2022 (08 November 2022)

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System) products.

The EcoStruxure EV Charging Expert products are load management, access management and supervision solutions for EV charging infrastructure.

Failure to apply the available remediations may risk potential unauthorized access to the product's web server, which could lead to tampering and compromise of the product's settings and accounts. Such tampering could lead to things like denial of service attacks, which could result in unauthorized use of the managed EV charging stations, service interruptions, failure to communicate with the supervision system and the modification and disclosure of the product's configuration.

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

November 2022 Update: The CWE for CVE-2022-22808 has been updated (marked in red). No additional action is required for customers who have already followed the remediation instructions provided below.

Affected Products and Versions

Product	Version
EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System): HMIBSCEA53D1EDB HMIBSCEA53D1EDS HMIBSCEA53D1EDM HMIBSCEA53D1EDL HMIBSCEA53D1ESS HMIBSCEA53D1ESM HMIBSCEA53D1EML	All versions prior to SP8 (Version 01) V4.0.0.13

Vulnerability Details

CVE ID: **CVE-2022-22808**

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

A *CWE-352: Cross-Site Request Forgery* vulnerability exists that could cause a remote attacker to gain unauthorized access to the product when conducting cross-domain attacks based on same-origin policy or cross-site request forgery protections bypass.

CVE ID: **CVE-2022-22807**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

A *CWE-1021 Improper Restriction of Rendered UI Layers or Frames* vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the web interface rendered within iframes.

Remediation

Affected Product & Versions	Remediation
EcoStruxure EV Charging Expert *All versions prior to SP8 (Version 01) V4.0.0.13*	Version SP8 (Version 01) V4.0.0.13 of the EcoStruxure EV Charging Expert product includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/62159-ecostruxure%E2%84%A2-ev-charging-expert/#software-and-firmware The installation procedure requires a reboot of the product in order to complete the update. After installation, the software version can be checked through the operation interface in the Updates tab.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

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 intended for that device.
- 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.

Acknowledgement

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2022-22808, CVE-2022-22807	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

About Schneider Electric

Schneider’s purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *08 February 2022*	Original Release
Version 2.0 *08 November 2022*	The CWE for CVE-2022-22808 has been updated (marked in red). No additional action is required for customers who have already followed the remediation instructions.

Product Security Office

Digitally signed by Product Security Office
Date: 2022.11.07 09:51:50 -05'00'