Schneider Electric Security Notification

EVlink Home Smart and Schneider Charge

8 October 2024

Overview

Schneider Electric is aware of a vulnerability with the potential disclosure of confidential information in its EVlink Home Smart and Schneider Charge charging stations.

This is not related to any of the customer personal data and potential disclosure cannot be exploited to abuse both products. This only relates to remote test equipment and test features that are removed from production units.

A remediation for affected charging stations has already been deployed to all connected units.

Affected Products and Versions

Product	Version
EVlink Home Smart	All versions prior to 2.0.6.0.0
Schneider Charge	All versions prior to 1.13.4

Vulnerability Details

CVE ID: **CVE-2024-8070**

CVSS v3.1 Base Score 8.5 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L

CWE-312: Cleartext Storage of Sensitive Information vulnerability exists that exposes test credentials in the firmware binary.

It is to be noted that this case does not allow any exploitation of the product as this information is related to remote test equipment and test features that are removed from the production units.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
EVlink Home Smart *All versions prior to 2.0.6.0.0*	For already connected products, version 2.0.6.0.0 of EVlink Home Smart includes a fix for this vulnerability and has been deployed to automatically upgrade all charging stations connected to the Wiser application. Make sure the charging station is connected to the Wiser application to ensure the new version is downloaded and installed. For new installations, a fix for this vulnerability is enforced through eSetup commissioning application. The installed firmware version can be verified through Wiser application (refer to the settings page for the charging station).
Schneider Charge *All versions prior to 1.13.4*	For already connected products, version 1.13.4 of Schneider Charge includes a fix for this vulnerability and has been deployed to automatically upgrade all charging stations connected to the Wiser application. Make sure the charging station is connected to the Wiser application to ensure the new version is downloaded and installed. For new installations, a fix for this vulnerability is enforced through eSetup commissioning application. The installed firmware version can be verified through either Wiser application (refer to the settings page for the charging station), or the third-party supervision application.

General Security Recommendations

We strongly recommend the following cybersecurity best practices.

- Device should only be used in a personal home network.
- Device should not have a publicly accessible IP address.
- Do NOT use port forwarding to access a device from the public internet.
- A device should be on its own network segment. If your router supports a guest network or VLAN, it is preferable to locate the device there.

- Use the strongest Wi-Fi encryption available in the home Wi-Fi network, such as WPA3 or WPA2/3 with protected management frames.
- Schedule regular reboots of your routing device, smartphones, and computers.
- Ensure that unauthorized individuals cannot gain physical access to your devices or regularly inspect the device for visual clues that may reveal a tampering attempt.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2024-8070	Simon PetitjeanSIMON PETITJEAN (independent security researcher)

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

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

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 1.0.0 08 October 2024	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.10.18 11:08:35 -04'00'