CYBER SECURITY ADVISORY

Terra AC Wallbox Authentication and Communication Vulnerabilities

CVE ID: CVE-2023-0863, CVE-2023-0864

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

All Terra AC wallbox product versions **less than or equal to** those listed below are affected.

Product Name	Product version	
Terra AC wallbox (UL40/80A)	**1.5.5**	
Terra AC wallbox (UL32A)	1.6.5	
Terra AC wallbox (CE)	Terra AC MID	1.6.5
	Terra AC Juno CE	1.6.5
	Terra AC PTB	1.5.25
	Symbiosis	1.2.7
Terra AC wallbox (JP)	1.6.5	

For further info on the portfolio please refer to the Terra AC wallbox product brochure at https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A2257&LanguageCode=en&DocumentPartId=&Action=Launch [1]

Vulnerability IDs

CVE-2023-0863, CVE-2023-0864

Summary

ABB is aware of private reports of a vulnerability in the product versions listed above. An update is available that resolves a privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could send a specially crafted message to the system node, allowing an attacker to execute actions and modify or read configuration settings of the product. An attacker could also eavesdrop during configuration or usage of the device.

Recommended immediate actions

The problem is corrected in the following product versions; apply the following update depending on product variant:

Terra AC wallbox (UL40/80A)	1.5.6	
Terra AC wallbox (UL32A)	1.6.6	
Terra AC wallbox (CE)	Terra AC MID	1.6.6
	Terra AC Juno CE	1.6.6
	Terra AC PTB	1.5.26
	Symbiosis	1.2.8
Terra AC wallbox (JP)	1.6.6	

In addition, the following mobile applications must be updated:

Charger Sync Mobile application version >= 1.9.3

(if applicable), TerraConfig Mobile application version >= 1.9.3

If updating via OCPP, the exposure is mitigated by having your charger updated to the latest firmware version, see above. Further information should be communicated to you by your CPO.

If updating via Bluetooth Low Energy, please update to the latest Charger Sync app version, i.e. 1.9.3 up, and upgrade your charger to the latest firmware available (see above depending on model). After the process is complete and after the mobile has successfully connected to the charger via the latest version of Charger Sync, the exposure to your charger will be mitigated. Should you receive a message on your app warning the communication was not successfully updated, please follow the link prompted in the message for further instructions.

ABB urges that customers apply the update as soon as possible.

Vulnerability severity and details

A vulnerability exists in the authentication and data transmission in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, allowing the attacker to use the product and modify or read configuration settings of the product. An attacker could also eavesdrop on data transmission if nearby while a legitimate user is using the system node.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

[1] The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2023-0863 Authentication Bypass

Authentication to access the AC wallbox via its Bluetooth Low Energy (BLE) channel can be bypassed, enabling unauthorized usage or configuration of a device. This would allow an unauthorized user to connect to the AC wallbox and act as a legitimate user, read or disclose stored charger configuration data, and change configuration of the device.

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	8.2 (High)
CVSS v3.1 Vector:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-0863

CVE-2023-0864 Plaintext Communication of Configuration Data

Configuration data is exchanged in plaintext and could be available to a nearby attacker if present during configuration or usage of the device via Bluetooth Low Energy (BLE).

CVSS v3.1 Base Score:	7.1 (High)
CVSS v3.1 Temporal Score:	6.6 (Medium)
CVSS v3.1 Vector:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-0864

Mitigating factors

Mitigating factors on nodes include

- Physical controls around the AC wallbox which limit access to the device's Bluetooth Low Energy range.

Refer to section "General security recommendations" for further advice on how to keep your system secure.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could send commands to a system node and read or write configuration of an affected system node.

What causes the vulnerability?

The vulnerability is caused by improper authentication in the Terra AC wallbox and data being communicated in plaintext.

What is Terra AC wallbox?

Terra AC wallbox is a Level 2 Electric Vehicle charger.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could send a specially crafted message to the system node, allowing an unauthorized attacker to use the product and read and modify configuration settings of the product. An attacker could also eavesdrop during configuration or usage of the device.

How could an attacker exploit the vulnerability?

A nearby attacker could try to exploit the vulnerability by sending crafted messages to an affected system node or eavesdrop on communications if present during usage or configuration. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

To exploit this vulnerability, an attacker would need to have physical proximity to an affected system node. If exploited locally, it could be possible for an attacker to configure the AC wallbox to connect to a remote OCPP backend.

Can functional safety be affected by an exploit of this vulnerability?

The maximum current parameter could be changed; software-defined limits are in place in case this parameter is set incorrectly. In addition, installation requires protective devices external to the Terra AC wallbox. Please refer to the installation manual https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A4972&LanguageCode=en&DocumentPartId=&Action=Launch [2]

What does the update do?

The update modifies the way that the AC wallbox and mobile applications communicate via Bluetooth Low Energy.

Furthermore, for software version 1.6.6, it raises OCPP 1.6J Security Events of type AttemptedReplayAttacks and places entries into the device security log in case unusual behavior is detected. This security event type is defined in [3].

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general purpose network (e.g. office or home networks).

Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.

Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.

Scan all data imported into your environment before use to detect potential malware infections.

Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.

Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.

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.

Acknowledgement

ABB acknowledges and thanks Andi Leach and Puck Meerburg who responsibly disclosed these vulnerabilities and provided valuable input on product improvements.

ABB also acknowledges and thanks Lionel R. Saposnik from Saiflow who also responsibly disclosed these vulnerabilities and provided valuable input on product improvements.

References

[1] ABB E-mobility, "The home of charging, Terra AC wallbox," [Online]. Available: https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A2257&LanguageCode=en&DocumentPartId=&Action=Launch.

[2] ABB E-mobility, "Installation Manual, Terra AC (BCM.V3Y01.0-EN)," [Online]. Available: https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A4972&LanguageCode=en&DocumentPartId=&Action=Launch.

[3] Open Charge Alliance, "Improved security for OCPP 1.6-J, edition 3 FINAL," 2022.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial release	2023-05-17