Advisory on vulnerabilities
Enel X Waybox Pro & Plus 3.0 charger

We inform you that Enel X Waybox Pro and Plus charger (3.0 versions)[1] firmware version before 2.1.1.0_JB3VU096A contains security vulnerabilities. These vulnerabilities do not pose any risk to personal data.

We have promptly fixed these vulnerabilities through a remote firmware update to avoid any potential attacks.

No further actions are required by you or end users to address these issues. All the Waybox connected to internet received this fix automatically. If the Waybox is not connected to internet, download Enel X Way mobile App from your app store and follow the instructions.

This document provides you with a description of all identified vulnerabilities and explains which type of information a malicious attacker could have gained access to before they were fixed. We are not aware of any real malicious attacks on any installed charger.

1. History

These security vulnerabilities were discovered by PCAutomotive (Abdellah Benotsmane, Anna Breeva, Artem Ivachev, Danila Parnishchev) and were confirmed by Enel X Way. Enel X Way and PCAutomotive have exchanged in a constructive manner on the identified vulnerabilities. According to our tests, an attacker exploiting the vulnerabilities on an unpatched charger could gain access to information stored on the charger, bypass charging restrictions set by the device owner, and cause denial of service on the charger. No personal data would be accessible during a potential attack.

We have promptly released new firmware that resolves all the identified vulnerabilities and we are updating remotely all affected connected chargers. No actions are required by you or the end users.

2. Affected Products

Enel X Waybox Pro 3.0 charger with firmware version before 2.1.1.0_JB3VU096A.

3. Description of the identified vulnerabilities

CVE-2023-29114: System logs disclosure

System logs could be accessed through web management application due to a lack of access control.

CVE-2023-29115: Denial of service via web management interface

In certain conditions a request directed to the Waybox Enel X Web management application could cause a denial-of-service (e.g. reboot).

[1] Enel X Waybox is part of the product portfolio of Enel X Way S.r.l.

CVE-2023-29116: PHP information disclosure

Under certain conditions, through a request directed to the Waybox Enel X web management application, sensitive information like Waybox OS version or service configuration details could be obtained.

CVE-2023-29117: Authentication bypass in Waybox Web Manager

Waybox Enel X web management API authentication could be bypassed and provide administrator's privileges over the Waybox system.

CVE-2023-29118 #1, CVE-2023-29119 #2: Unauthorized SQLite injection

Waybox Enel X web management application could execute arbitrary requests on the internal database.

CVE-2023-29120: Unauthorized remote command execution

Waybox Enel X web management application could be used to execute arbitrary OS commands and provide administrator's privileges over the Waybox system.

CVE-2023-29121: Exposed TCF agent service

Waybox Enel TCF Agent service could be used to get administrator's privileges over the Waybox system.

CVE-2023-29122: Incorrect file ownership of privileged service's libraries

Under certain conditions, access to service libraries is granted to account they should not have access to.

CVE-2023-29125: Heap overflow in CM_main.exe binary

A heap buffer overflow could be triggered by sending a specific packet.

CVE-2023-29126: Insecure loose comparison

The Waybox Enel X web management application contains a PHP-type juggling vulnerability that may allow a brute force process and under certain conditions bypass authentication.