**Advisory on vulnerabilities**
**Enel X Juicebox 2.01 (40A) charger**

Enel X has resolved a vulnerability affecting JuiceBox 2.01 (40A) chargers running firmware 1.0.46 or earlier. The issue does not expose personal data of users and does not have any cyber and/or safety impact.
The patched firmware 1.0.47 has been remotely deployed to all chargers connected to the internet; no action is required for units that have already received the update.
Devices that have not been updated through remote rollout can be updated manually. If assistance is needed, customers may contact Enel X Customer Service at emobility.globalcontrolroom@enel.com.

## 1. History

The Zero Day Initiative (ZDI) reported the issue under ZDI-26-041, associated with CVE-2026-0778. A potential attacker on the same local network could on unpatched chargers exploit the unauthenticated Telnet service on TCP port 2000 to execute code remotely.
Enel X confirmed the finding and released firmware 1.0.47, which removes this vulnerability.

## 2. Affected Products

Enel X JuiceBox 2.01 (40A) charger with firmware version prior to 1.0.47.

## 3. Description of the identified vulnerability

***CVE-2026-0778 – Unauthenticated Telnet Access***
A Telnet service exposed on port 2000 allowed network-adjacent access without authentication. Potential impacts included:

- Execution of arbitrary commands with service-level privileges

The issue was limited to local-network access and did not involve personal data exposure.

## 4. Mitigation

Enel X has released firmware version 1.0.47, which disables the unauthenticated Telnet service.

All devices connected to the internet have already received the update automatically.

For units not updated automatically, customers must use the standard manual update procedure to install version 1.0.47. If support is required during the manual update, customers may contact Enel X Customer Service for assistance.