Vestel Cyber Security Notification

20.02.2025
VSA-1_R2

Overview

Vestel is aware of vulnerability in its EVC04 AC Charger products.
EVC04 is an AC charger that supports 7 – 22kW power with connectivity features such as WIFI, ethernet and LTE.
Failure to apply the fix provided below may risk a denial of service and partial loss of integrity of the charger, which could result in disruption of its operations.

Effected Products and Versions

Product	Details
EVC04-AC*SW*****	Any version connected to open internet and have default web configuration interface credentials.
EVC04-AC*SWL*****	
EVC04-AC*SL*****	
EVC04-AC*S*****	

Vulnerability Details

Any IoT device which are connected to open network can be discovered by any unauthorized passive reconnaissance application, such as EVC04.
An attacker may then gain access to the web configuration interface by using the default username and password resulting in taking control of the charger.

Mitigations

Avoid using open network:

- Use secure methods like Virtual Private Networks (VPNs) for remote access. Regularly update VPNs to their latest versions and ensure that connected devices maintain strong security measures.
- Reduce network exposure for applications and endpoints. Only make them accessible via the Internet if specifically designed for and required by their intended use.

Login Credentials Management:

- Force end user to revise the factory default set username and password of webconfig page.
- Remove any printed documents such as installation guide, instruction book, quick start quide from web where login credentials are featured.

Vestel strongly suggests that customers using the related AC chargers shall upgrade to V3.187 or any upper version.

General Security Recommendations

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- 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.
- Keep all nodes updated with the latest software, operating system, firmware patches, antivirus definitions, and firewall settings.

Vestel Mobility
Ege Serbest Bölgesi Akçay Cad.Ayfer Sok. 144/1,
Gaziemir, İZMİR /TÜRKİYE
Tel: +90 236 233 01 31
www.vestelinternational.com