EV Charger Pentesting

In-Depth Technical Security Assessments of Electric Vehical (EV) Chargers.

The rapid growth of electric vehicles (EVs) has led to an equally rapid expansion of charging infrastructure. Modern EV chargers are highly connected systems that expose multiple interfaces, including web portals, mobile applications, NFC, Bluetooth, Wi-Fi hotspots, and cloud backend services. While these features improve usability and remote management, they also significantly increase the attack surface of charging stations.

A compromised EV charger can lead to financial fraud, unauthorized charging sessions, service disruption, or attacks against connected backend infrastructure. These risks highlight the growing importance of penetration testing and security assessments for EV charging infrastructure.

Preparation

The preparation phase of an EV charger penetration test starts with precise scoping to define which systems and interfaces are included in the assessment. In many cases, backend infrastructure and cloud services are excluded to keep the test focused on the charging station itself. During the kickoff meeting, the customer's specific security concerns and priorities are captured, this includes gathering questions the assessment shall provide answers for. For example, if backdoor accounts or default credentials are present on the device, or concerns about undocumented maintenance interfaces, firmware integrity, or the resilience of wireless communications. These inputs are complemented by the most critical attack scenarios relevant to the deployment context, including physical tampering, network-facing service exploitation, wireless interface abuse, and OCPP layer manipulation. The resulting priority list directly shapes the test plan, ensuring that the assessment addresses what matters most to the customer.

Technical Assessment

- Hardware Inspection and Memory Extraction
- Reverse Engineering of proprietary Protocols and services
- Fuzz Testing of Protocol Implementations
- Mobile App testing
- Web Interface testing

The technical assessment begins with an attempt to gain local access to the device, in order to move from a black-box approach toward a grey- or white-box assessment. This is achieved either through opportunistic access, such as exposed services or misconfigurations that allow privilege escalation, or through physical means such as UART console access or flash memory dumping. Elevating the level of access early in the engagement significantly increases the depth and coverage of the overall assessment. Once access is established, the team systematically works through the agreed attack vectors and priorities defined during the kickoff, covering areas such as network-facing services, wireless interfaces, physical attack surfaces, authentication mechanisms, and inter-component communication. Each finding is evaluated in the context of the customer's specific deployment and the concerns raised during the preparation phase, ensuring the assessment remains focused and actionable throughout.

Typical Challenges

- Extracting Firmware / Gaining Local access
- Monolithic Architectures
- Limited Scope

Technical EV charger assessments come with several recurring challenges. Physical memory extraction is particularly demanding — accessing flash storage without damaging the board or triggering tamper protection requires both precision and experience. When direct extraction is not feasible, intercepting firmware updates in transit is an alternative, though these are frequently encrypted or delivered over proprietary protocols. Many charging stations run monolithic firmware architectures, where tightly coupled components make reverse engineering significantly more difficult and time-consuming. The OCPP communication layer adds further complexity, as vendor-specific implementation deviations often conceal security-relevant behavior. Finally, backend infrastructure and cloud-based charge management systems are frequently out of scope due to vendor or operator restrictions, despite playing a central role in the overall attack surface.

Common Vulnerabilites

- Command Injections in the Web,
- UART Access,
- Backdoor Authentication (accounts, tokens),
- Memory Corruptions
- Charge port network access

Across EV charger assessments, certain vulnerability classes appear regularly. Physical access to the debug interface frequently yields significant results, exposed UART consoles often provide unauthenticated shell access, while unlocked bootloaders or accessible recovery modes allow full firmware extraction and modification. Charge ports often enable attackers to access the internal management interfaces. The management web interfaces hosted directly on the charging unit are a recurring source of critical findings, most notably command injection vulnerabilities stemming from unsafe input handling. Hardcoded or default credentials represent another common weakness, affecting both administrative interfaces and backend communication. Further proprietary protocols and services are prone to memory corruption vulnerabilities.

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Pentest of an OT Infrastrucutre or an IoT/IIoT/Embedded Device,

get in touch with us: office@cyberdanube.com

This Whitepaper has been inspired by real word projects.