TEST REPORT ON
CYBER SECURITY ISSUES AC AND DC CHARGING STATIONS

RESEARCHING AN
D TESTING SMART
AND SUSTAINABL
E CHARGING

Wilco van Beijnum, Harm van den Brink and Paul Broos | May 2025 | Version 1.0

Table of contents

SUMMARY

ELAADNL RESEARCH UNCOVERS SYSTEMIC CYBER SECURITY ISSUES IN CHARGING STATIONS

Over the last year, ElaadNL has tested the cyber security of dozens of charging stations. During the testing, systemic issues were uncovered to which many charging stations are vulnerable. In this report, we will provide an overview of common vulnerabilities and discuss how we could apply this knowledge to improve the cyber security of the charging infrastructure.

ElaadNL performs various cyber security tests on both public and private charging stations provided to the ElaadNL Testlab. In these tests, we focus on three attack vectors. Firstly, we discovered vulnerabilities related to the communication over the charging cable, as internal services can be exposed through this interface. Secondly, the network connections of charging stations frequently rely on outdated services or custom software with exploitable weaknesses. Lastly, physical access to ports and connectors inside the charging station can provide unauthorized access to internal systems. Each of these scenarios underscores the critical need for improved security practices in charging infrastructure.

In this exploration, we will provide a technical description of the types of vulnerabilities we have commonly encountered. This information is especially relevant for those developing charging stations but can also be useful to consider for those procuring or operating charging stations. We will focus on attack vectors directly applying to charging stations. It is noteworthy that there are other attack vectors to take into consideration, such as those targeting cloud infrastructure, that fall outside the scope of our testing.

While the vulnerabilities described might seem limited to individual charging stations at first, the impact of these vulnerabilities should not be underestimated. Taking over a few charging stations can already have a significant impact on the mobility of a single company. Furthermore, access to a single charging station can be used to gain access to the internal network of the manufacturer or charge point operator and allow an adversary to attack other devices in this network. The increased knowledge gained on the functioning of the charging station after exploiting it can also allow an attacker to uncover further vulnerabilities. Once an attacker has gained control over a larger number of charging stations, they could install ransomware or even destabilize the power grid and cause blackouts.

CHAPTER 1

THE CHARGING CABLE

ATTACK SCENARIO

DC charging stations and certain AC charging stations, such as those supporting Plug-and-Charge (PnC) or Vehicle-to-Grid (V2G), use Ethernet communication to exchange messages with the EV. These messages, defined in the DIN-SPEC-70121 or ISO-15118 standards, are transmitted over the charging cable via the HomePlug GreenPHY powerline protocol. This high-level communication, known as HLC, is used to negotiate charging parameters. If services on the charging station are not properly configured, they may be exposed on this Ethernet interface, making them accessible to the EV.

METHODOLOGY

To investigate whether this issue occurs on any charging stations, we have developed a testing box that can simulate a car. This box uses a HomePlug GreenPHY modem and a modified version of SwitchEV's Josev software to communicate with the charging station and simulate the HLC that a car would produce.

COMMON VULNERABILITIES

Exposed services on the charging cable

We utilized the previously described DIN-SPEC-70121/ISO-15118 testing box to investigate around twenty different DC charging station models from various manufacturers, as well as an AC charging station supporting ISO-15118. Since the HLC uses Ethernet, we can use existing tools such as Nmap to perform a port scan on the IP address of the charging station. Using this methodology, we discovered that around half of the investigated charging stations expose internal services on the charging cable's HLC interface. Almost all investigated charging stations with exposed services exposed an SSH service. Additionally, we identified charging stations exposing a Telnet server, an MQTT server that was not password-protected, custom services, and even HTTP services running configuration web interfaces. By exploiting vulnerabilities in these services, or by abusing insecure or default credentials, it is thus feasible that an attacker might gain access to a charging station via the charging cable. We will go into more detail on possible vulnerabilities in these services in the next section on network interface vulnerabilities.

If you are interested in learning more about this vulnerability, we would like to refer to our blog "Hacking EV charging stations via the charging cable".

Vulnerabilities in the HLC service

Aside from exploiting exposed internal services, an attacker could also attack the service responsible for the HLC using DIN-SPEC-70121 or ISO-15118.

TrendMicro published research in 2021 that showed the possibility of hacking a charging station using the Log4shell vulnerability in the Log4j Java dependency. In our investigations, we did not find any charging stations using Java. Therefore, we believe that the impact of this potential vulnerability is likely limited.

We identified that most HLC services are native applications. Because of this, these services could be vulnerable to buffer overflow attacks. Furthermore, these services might contain further logic errors or injection vulnerabilities that could be abused. Although we have not investigated the prevalence of these kinds of errors in the HLC services, we plan to investigate this in the future. The researcher P. Khunt has developed a scanning tool for this purpose as his master thesis, which currently focuses mostly on testing the EV as opposed to the charging station. However, he did not test the tool on actual vehicles.

Aside from directly attacking the HLC service, it is also possible to attack the physical layer of the HLC communication. Köhler et al. have shown in their 2023 study that a jammer can be used to disrupt communication between the charging station and EV, interrupting the charging session.

CHAPTER 2

NETWORK INTERFACE

ATTACK SCENARIO

Charging stations, especially public ones, are often connected to the Internet via a mobile connection, Ethernet or Wi-Fi. These connections can be used by an attacker to gain access to the charging station. Although properly configured charging stations are typically behind a private APN, firewall, or NAT to prevent direct access via the Internet, we have identified many charging stations where this is not the case. Attackers could also gain access to the network of charging stations through physical means or through vulnerabilities in the CPO's or manufacturer's infrastructure, or even via the charging cable, as previously described. In our tests, we assess the security of services exposed through open ports, as well as the security of communication between charging stations and backend servers, checking for vulnerability to man-in-the-middle attacks. Aside from these network connections, some charging stations might also have a Bluetooth interface available to update its configuration, which can also be an entrypoint for an attacker.

METHODOLOGY

To investigate the security of the network interface of the charging station, we typically first identify open ports, and the services running on these ports. If we can determine any used software, we check for known vulnerabilities. For web servers, we test for common web server vulnerabilities, such as the ones described in the OWASP Top 10, using both automated and manual testing. Additionally, we examine any network traffic originating from the charging station. Here, we investigate whether encryption is used, and if certificates are properly validated.

If the charging station can be configured via a smartphone app, we can also investigate the network traffic from this app. This is especially relevant when communication happens over Bluetooth.

To speed up testing, we have developed a cyber security quickscan tool tailored to charging stations. This tool combines existing tools, such as Nmap and Mitmproxy, with self-developed scans to identify certain vulnerabilities in charging stations. This tool can, for instance, automatically investigate the network traffic of a charging station, identify certain common web vulnerabilities, and identify running software and known vulnerabilities in this software. After scanning a charging station, the results provide a clear overview of the attack surface of the charging station, and potential weak points that can be further explored manually.

COMMON VULNERABILITIES

Commonly exposed services

Network scans revealed that almost all charging stations have some services exposed on their Internet-facing (WAN) network interface, often running outdated software with known vulnerabilities. Almost all charging stations expose an SSH service, with used versions dating as far back as 2017. Many also provide HTTP web interfaces for configuration, which frequently lack proper security, particularly around user input

filtering. Aside from this, we also find other services, such as Modbus/TCP, which is usually used to allow for remote control of a charging station. However, if not properly secured, Modbus/TCP can be exploited to read and write sensitive data.

User input filtering and injection vulnerabilities

Although extensively documented online, injection vulnerabilities remain common in charging station web interfaces, ranging from XSS and SQL injection to OS command injection. These vulnerabilities highlight the importance of proper input filtering and escaping. As most web interfaces or OCPP services run with root access, a command injection vulnerability can give an attacker full control over the charging station, allowing them to manipulate the functioning of the charging station, corrupt its firmware, or deploy ransomware.

SQL injection, though often less severe than command injection, can still have significant impacts, such as bypassing login screens or accessing sensitive files and data such as user credentials, Wi-Fi passwords and charging card IDs. This is especially relevant when the vulnerability can be exploited without requiring authentication.

XSS vulnerabilities are typically less severe but can be exploited to steal session tokens or other sensitive data, especially in combination with phishing attacks. The lack of CSRF protection in many stations further increases the risk of these attacks.

A final concern related to user input filtering is server-side request forgery (SSRF). There are several cases where the charging station uses a user-controlled URL, for example for the OCPP address, a URL to display on the charging station, or an URL to upload to or download from in an OCPP request. When not properly restricted (for example, allowing the *file://* schema), these URLs could trigger unwanted behavior in the charging station.

Uploading and downloading files

Many charging stations allow file uploads for tasks like backups or firmware updates. If these files are not properly handled, the station's integrity can be severely compromised. While firmware updates are usually encrypted or signed, we have been able to exploit charging stations that did not properly validate the signature of a firmware update. Furthermore, backup files often lack integrity checks and encryption, making them especially vulnerable. We were able to exploit this weakness on several charging stations by adding new files in backup archives or modifying existing files, leading to overwriting of configuration files or uploading of binary files, giving full control over the charging stations.

Authentication and authorization

When charging stations have web interfaces for configuration, sensitive information should be protected behind a secure login screen. However, we found several instances of broken access control, where pages like logs and configuration backups were accessible without authentication, exposing sensitive data such as charging card IDs and credentials.

Even with proper authorization, security is ineffective if authentication can be easily bypassed. We have seen many cases where the same default password, often found in manuals or guessed from common patterns, is used on all charging stations. Additionally, operators are rarely forced to change this default password during provisioning, causing countless deployed charging stations to potentially still use this default password. Some

stations use passwords based on serial numbers or MAC addresses, which can be brute-forced or found during physical attacks.

We also discovered that many manufacturers retain maintenance access via SSH login or a hidden web interface account. Although, in case of SSH, keypairs are frequently used, which are principle secure, improper storage or leakage of the private key could compromise all stations. In cases where password authentication is used, we have even found cases where this password is stored in plaintext or as a weak hash, enabling attackers to access all charging stations if they can extract and crack the password.

Memory management

Many charging stations use native binaries, such as CGI or web server binaries for the configuration interface or background processes like the OCPP or ISO-15118 communication client. Proper memory management is crucial to prevent buffer overflow vulnerabilities, which can crash applications, causing denial-of-service attacks if the service doesn't auto-restart. In the worst case, they can allow arbitrary code execution. Although not our main research focus, we identified various buffer overflows, indicating that these vulnerabilities are still common.

Extracting information from firmware

Most firmware update files are cryptographically signed, preventing unauthorized modifications. However, if the firmware is not encrypted, sensitive information can still be extracted. We have successfully extracted password hashes, plaintext passwords, and API credentials from firmware files. Additionally, access to scripts and binaries running on the charging station, such as those for the web server, enables us to identify vulnerabilities by reviewing script code or reverse-engineering binaries. Using this approach, we discovered many vulnerabilities, among which various command injection vulnerabilities that resulted in full root access on several charging stations.

Network traffic and encryption

Charging stations often communicate with backend servers over the Internet, transferring data such as payment details, station status, and firmware updates. Ideally, this communication uses a secure OCPP connection. However, many manufacturers use proprietary protocols, sometimes fully replacing OCPP, especially with consumer stations controlled via an app or website. If not properly secured, vulnerabilities in these communication channels could even lead to the compromise of all stations from a manufacturer.

While encrypted TLS connections are standard for websites nowadays, many charging stations fail to properly encrypt communication with their servers. Some use encryption but don't validate TLS certificates, or even use no encryption at all, allowing attackers to intercept or modify traffic via man-in-the-middle attacks. This could allow an attacker to manipulate firmware updates, stop charging sessions, or steal sensitive data. Unencrypted traffic could also aid an attacker in finding vulnerabilities in the backend server.

In addition to external communication, many charging stations have unencrypted local services, such as configuration interfaces that only support HTTP. If an attacker intercepts this traffic, they could gain access to sensitive information or even modify the station's configuration.

CHAPTER 3
PHYSICAL ACCESS

ATTACK SCENARIO

An attacker might also be able to exploit a charging station by gaining physical access, for instance by (forcefully) opening a charging station. Inside, they can connect to internal ports such as Ethernet or USB to gain access to internal services, or connect to debugging connectors such as UART or JTAG. Furthermore, memory chips could be read to gain access to the firmware of the charging station.

METHODOLOGY

By opening a charging station, we can identify exposed external ports, such as Ethernet ports for Internet or internal communication. Furthermore, USB connectors can sometimes be used to escape the user interface of the charging station. Finally, debugging interfaces such as UART or JTAG can be found, which are sometimes even marked as such, for example using "RX" and "TX".

We can connect a laptop to the Ethernet ports, peripherals to the USB connectors, or a USB converter to UART or JTAG connectors to investigate the security of these connectors. Sometimes, these physical connectors allow for full access to the device.

Although a physical attack may seem challenging, it can often be quite straightforward to execute, only requiring a screwdriver, a common key, or the creation of a small hole. Access to the OS, bootloader or flash chip of the charging station using one of these methods can also allow an attacker to dump the firmware of the charging station, which can be analyzed to find vulnerabilities that are exploitable on a larger scale, such as the ones described previously. This way, physical access to only one charging station is required, which could also be purchased by the attacker for the purpose of finding other vulnerabilities.

COMMON VULNERABILITIES

Internal Ethernet ports

In the previous chapter, we examined the security of WAN ports on charging stations. Many stations also use Ethernet for communication between internal components, such as the main controller and the HLC or user interface controller. If unused LAN ports are not disabled, an attacker could connect to this port, gaining access to the internal LAN network without disrupting component communication. In many cases, SSH is running on internal components. Furthermore, this could provide access to services such as the charging station's configuration web interface without needing access to the external network of the charging station.

USB ports

Attaching a keyboard to an exposed USB port may allow for access to other parts of the operating system. For example, we can use common key combinations, such as *Alt-Tab* or *Alt-F4*, to escape the current application or gain access to a terminal. In some cases, we were able to gain access to a terminal screen but were still prompted for login credentials.

In other cases, we could, for instance, gain access to the internal settings of the charging station using *Alt+Tab*. It might also be possible to interrupt the boot process and enter the bootloader.

Access via debugging ports

Many charging stations provide debugging access through ports like UART and JTAG. UART connectors often provide access to the OS. We have seen stations where UART access required login credentials, while others gave immediate shell access. JTAG offers even deeper access, allowing direct debugging of the processor, facilitating memory manipulation, extraction of sensitive data, and bypassing firmware security measures. So far, we have only tested labeled UART connectors, and plan to perform more extensive tests of UART and JTAG in the future.

Reading flash storage

Charging stations often store sensitive data, including charging card IDs and configuration details like passwords, on embedded flash storage or removable SD cards. An attacker can easily access and clone SD cards. For embedded flash storage, desoldering the chip allows access to its data, provided it is not encrypted, enabling firmware analysis and access to sensitive information. Our current research in this area shows promise for uncovering more vulnerabilities in a charging station's firmware.

CHAPTER 4
OTHER ATTACKS

At ElaadNL, we mostly focus on investigating the cybersecurity of the charging station itself, as described in the previous chapters. However, there are still other cyber security issues in the charging infrastructure domain. We will briefly mention these below.

CHARGING CARDS

Charging cards used for authentication are highly insecure, as authentication relies solely on the card's UID, making them easy to clone via skimming. Charging stations and backend servers often store lists of authenticated UIDs, which attackers can exploit to create cloned cards and charge EVs at others' expense.

BACKEND INFRASTRUCTURE

Although ElaadNL has so far not specifically investigated the security of backend infrastructure, we are aware of several vulnerabilities that were identified in several backend servers. These vulnerabilities disclosed sensitive information such as charging card UIDs or allowed control over other charging stations. As these servers are often publicly accessible via the Internet, it is vital that they are well secured and protected, especially since taking over this infrastructure often gives an attacker control over all connected charging stations.

CHAPTER 5

CONCLUSIONS AND FUTURE DEVELOPMENTS

CONCLUSION

The cybersecurity of the charging infrastructure sector still requires significant improvement. While a few manufacturers demonstrated strong security, critical security vulnerabilities were found in many other charging stations. This highlights a lack of focus on cybersecurity by some manufacturers, although we have seen several manufacturers quickly address vulnerabilities once we notify them, demonstrating a proactive approach to improving security. As the number of charging stations grows, protecting this infrastructure against cyberattacks is essential to prevent potentially severe societal impacts. As smart charging becomes more prevalent, this concerns only further increases. At ElaadNL, we are committed to raising awareness among manufacturers, CPOs, and other stakeholders. Strengthened regulations and standards can further drive progress in securing this vital infrastructure.

TECHNICAL ADVICE

Developing or managing secure charging stations is a complex task. Manufacturers and CPOs must ensure both the charging stations, and their surrounding infrastructure, are robust against cyber threats. Below, we give some key recommendations.

Advice for manufacturers of charging stations

Developers and designers of charging stations should familiarize themselves with requirements like the ElaadNL/ENCS requirements, and common vulnerabilities such as the ones described in the OWASP Top 10 and OWASP IoT Top 10, focusing on areas such as authorization, input validation, and using unique passwords for each charging station. Special attention should also be given to memory management when developing native binaries to prevent vulnerabilities like buffer overflows. Firmware updates should be signed and encrypted. Finally, we recommend conducting a full pentest of your charging station by a party that specializes in charging station or embedded device security, such as ENCS.

Advice for CPOs

CPOs should ensure that charging stations and related infrastructure meet security standards like the ElaadNL/ENCS requirements. Furthermore, special care should be taken in securing backoffice software. Regularly conducting pentesting is crucial for identifying weaknesses. Furthermore, we recommend using unique passwords, with multi-factor authentication where possible, and network segmentation to limit the impact of potential breaches.

CHAPTER 6

LEGISLATION

As the potential impact of a large-scale cyber-attack on charging stations is significant, legislation is slowly catching up to place more strict requirements on the cyber security of these devices.

The Dutch cyber security law had an interim adjustment in October 2023 by including Charge Point Operators that operated chargers with a total sum of maximum power of 300 megawatt as part of the vital infrastructure. As a result, these CPOs now have an obligation to report incidents, with a possible effect of 100 megawatt or more. This seemed like a minor change, with no direct force on increasing the cyber security level, but getting insights into possible attacks on those large operators is very valuable.

In the EU-NIS2, the updated version of the previous NIS (Network and Information Security) directive, now also includes under Annex I, sectors of *High Criticality,* "*Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider*". This will mean that the CPOs and/or others operating a charge station are obliged to have proper cyber security in place, as well as the obligation to report any incidents to the designated authorities. In The Netherlands, the NIS2 will be implemented in the Cyberbeveiligingswet which will come into force in autumn 2025.

Also, later this year, the extended article 3.3 of the EU Radio Equipment Directive will come into force. This includes requirements for network integrity, personal data and privacy protection and fraud prevention. The technical specifications have been described in the norm EN 18031.

The EU Network Code on Cyber Security code is specifically for the electricity sector and aims to secure international electricity flows. The code covers all parties that may pose cross-border cyber risks for this purpose, including Charge Point Operators (CPOs). Companies are designated by the competent authority based on a periodically conducted risk assessment. If this is the case, stricter requirements will apply.

Finally, the EU is preparing a new Cyber Resilience Act. This act has a broad horizontal effect and mainly affects charging point manufacturers. They must support their complete solution, i.e. including app and cloud environment, for the full lifetime of their product.


Elaadnl