National Test Institute for Cybersecurity

Security Analysis of the Swiss Charging Infrastructure for Electric Mobility

A Technical Assessment

v1.0 / 15.11.2023
November 15 2023, 08:00

Document ID	NTC-20231115-1-en
Subject	Security Analysis of the Swiss Charging Infrastructure for Electric Mobility
Version	v1.0 / 15.11.2023
Date	November 15 2023, 08:00
Classification	Public
Authors	Patrik Fabian, Dilip Many, Raphael M. Reischuk, Fabio Zuber
Responsible	Tobias Castagna

Table of Contents

Changes

Version	Date	Changes
1.0	2023-11-15, 08:00	Initial document

1 Management Summary

1.1 Initial Situation and Background

The number of electric vehicles on Switzerland's roads is growing rapidly, and this trend is not expected to change any time soon. Many vehicle manufacturers have announced that they will no longer produce vehicles with combustion engines in the near future - partly because in many countries they are unlikely to be licensed for road use in a few years' time. Hence, a reliable charging infrastructure will be required to realize this transition in road transport. This infrastructure is currently being built in Switzerland, Europe and in many other regions of the world.

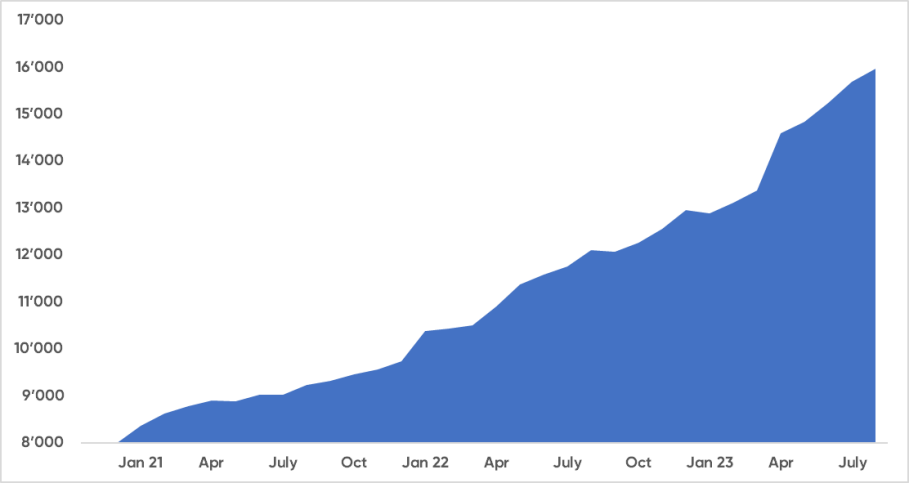

Figure 1: Number of charging stations in Switzerland. Source: Swiss eMobility: [13]

There are a variety of factors that make the public charging infrastructure particularly vulnerable to cyber attacks. Compared to the conventional gas station infrastructure, it is significantly more digital and connected. The charging points are computers which are connected to the Internet. They can be controlled using apps and both billing and maintenance is carried out via the centralized servers of the operators. Large-scale attacks against a variety of charging stations and the Swiss power grid are conceivable due to the high degree of connectivity. Physical proximity to the charging station is not required for a successful attack.

Unlike traditional energy infrastructure, this technology is relatively new and still evolving. It is therefore not an established technology that is widely known, tried and tested. The driving forces in this field are a large number of innovative start-ups that have emerged in recent years. Naturally, these start-ups are strongly focused on the fastest possible time to market and a high market penetration. Cybersecurity tends to get in the way and is often given a low priority. It has been assumed, and results confirm, that their products and connected infrastructure are currently not sufficiently tested for vulnerabilities.

The National Test Institute for Cybersecurity NTC tests precisely products and networked infrastructures relevant for the Swiss society that are not, or insufficiently, tested. The tests are

carried out on the NTC's own initiative and with its own resources in the interest of Swiss society. With this report, the results of this review are made available to the public.

The review focuses on risks that have a significant impact on the security of the Swiss society. Examples include vulnerabilities that could allow attackers to disable a large part of the charging infrastructure for multiple days or weeks, or to cause a large-scale power outage. Vulnerabilities that do not have a significant impact on our society are currently not focused on. An example in this case would be a vulnerability that allows attackers to charge at a third party's expense. Although this is unpleasant for the individual affected, it does not pose a threat to the Swiss society.

The authors would like to explicitly emphasize that the results of this report are not intended to undermine electric mobility. On the contrary, the aim is to point out potential vulnerabilities in this early expansion phase so that these can be addressed as early as possible and a robust and effective charging infrastructure can be built and operated in Switzerland.

1.2 Assessment Summary

One of the main risks is that much of the industry is still using the outdated version 1.6 of the common OCPP protocol. OCPP stands for Open Charge Point Protocol and is a manufacturer-independent communication protocol for charging station management, billing and monitoring. Protocol version 2.0, which adds important additional security features, has been available for several years. However, the de facto standard is OCPP version 1.6 from 2015, even though important security features are missing entirely or optional. As a result, the communication between the charging station and the backend is usually unencrypted, the authentication of the charging station to the backend is insufficient, there are no compulsory monitoring or logging options, and the update mechanism for the charging station firmware can be considered insecure.

Figure 2: Comparison of the OCPP versions. Source: Open Charge Alliance [9]

Besides the above-mentioned risks in connection with OCPP which affect a large part of the industry, a wide number of vulnerabilities were identified that affect individual manufacturers and products. Most of these vulnerabilities were identified in the backend systems and not in the charging stations themselves, as the review focused on the former. Vulnerabilities in backend systems have been classified as more critical, as they are more scalable and allow an attacker to target a large number of consumers remotely with little effort.

In most cases, there are easily detectable and exploitable vulnerabilities that can be identified at an early stage using automated tests. This suggests that the systems are not being sufficiently tested for vulnerabilities. The most frequently identified systems were those that either should not be accessible via the Internet at all, or that revealed more information than necessary due to a misconfiguration. For example, multiple unprotected configuration files were identified, that contained credentials and other sensitive information. Other vulnerabilities can be traced back to obsolete software, suggesting inadequate patch management.

SQL injection vulnerabilities have been identified with surprising frequency. This is a critical vulnerability class which was widespread in the past but has become less common in recent years due to modern development frameworks and increasing awareness among developers. In the OWASP Top 10 of 2017, injection vulnerabilities were still in first place [10]. Since 2021, this vulnerability class has dropped to third place - even if the widespread cross-site scripting (XSS) attacks are now included in that class [11]. This may be an indicator that certain good programming practices are not yet sufficiently established in the charging infrastructure industry.

Overall, around 30 manufacturers and operators were notified of vulnerabilities. Fortunately, these vulnerabilities were generally rectified within a few hours or days. By contrast, it was the reachability of the affected organizations that proved to be difficult and time-consuming.

While the responsible organizations are easy to find in most cases, it is significantly more difficult to identify and reach the responsible individuals within the organizations. A vulnerability disclosure policy, as is recommended by the NCSC [4], would greatly simplify and expedite the reporting of vulnerabilities. Unfortunately, such policies were not implemented by any of the organizations contacted.

Further details on the identified risks are listed in Section 3.2 on Page 12.

1.3 General Recommendations

The following general recommendations for the industry can be derived from the results of this assessment:

- The latest version of the OCPP protocol should be supported and used.
  - **OCPP 2.0.1 by default:** All new charging stations and OCPP backends should only use OCPP version 2.0.1 or newer.
  - **Deprecation of OCPP 1.6:** The Open Charge Alliance, which defines the OCPP standard, should label old and insecure versions of the protocol as deprecated and advise against their use.
- Secure programming practices should be adopted to prevent vulnerabilities such as SQL injection and cross-site scripting (XSS).
  - **Security awareness:** Raising awareness of security risks among developers during design, development and operation.
  - **Use of modern frameworks:** Modern frameworks often provide built-in methods for the secure implementation of a feature.
  - **Code reviews:** Frequent reviews of the source code for proper functionality and security.
  - **Data validation:** Implementation of comprehensive input checks and validation mechanisms to ensure that user inputs are securely processed.
- The attack surface of the systems should be reduced using hardening measures.
  - **Secure handling of credentials:** Credentials should not be part of the source code, nor publicly accessible in configuration files.
  - **Disabling of developer tools:** Developer tools should be disabled or restricted in productive systems.
  - **Prompt installation of security patches:** Promptly installing security patches is an important step in closing potential vulnerabilities and increasing a system's resilience against threats.
- Ability to report security vulnerabilities by ethical hackers should be improved.
  - **Implementation of security.txt:** Provide contact details on the system in order to send security notifications. The NCSC has published a bulletin on this [2].
  - **Vulnerability disclosure policy:** Policies created by organizations to regulate the process of reporting vulnerabilities. The NCSC has published a guide for companies and organizations for this purpose [4].
  - **Setting up a bug bounty program:** Increases the incentive for ethical hackers to look for vulnerabilities and report them responsibly.

- To authorize the charging process with RFID cards, a method based on asymmetric cryptography should be used, which makes copying cards more difficult.
  - **Use a method based on asymmetric cryptography:** Instead of simply reading the UID of the RFID card, a method based on asymmetric cryptography should be implemented. The VDE application rule *VDE-AR-E-2532-100* [14] is already supported by some manufacturers and could be a potential solution.

The details of the vulnerabilities detected and the associated recommended countermeasures have been communicated confidentially to the affected organizations as part of the responsible disclosure process [5]. An anonymized list of findings can be found in the appendix on Page 10.

1.4 Context

The review was carried out at the initiative of the NTC. The NTC provided the resources required for the review and determined the objectives, scope and framework conditions. The manufacturers and operators concerned did not have any influence on the review. There is no external contractor.

The review took place between May and August 2023 and was mainly carried out by a core team of three NTC test experts. In total, around 90 working days were spent on research, analysis, testing, documentation, notification and advice to the around 30 organizations concerned.

Only products and networked infrastructures which are accessible via the Internet or otherwise publicly available were tested. No tests were carried out on manufacturers' and operators' internal networks or non-public systems.

Further details on the scope and limitations are listed in Section 2 from Page 7.

2 Scope and Limitations of the Security Analysis

This section describes the scope of the security analysis performed. Further, the self-imposed, technical and the resource-related limitations are described. This is followed by an overview of the most important points, including a detailed explanation.

2.1 Overview of the Scope of the Analysis

As part of this analysis, the National Test Institute for Cybersecurity NTC investigated the security situation of the charging infrastructure for electric mobility. In this process, the focus was on infrastructure that is accessible via the Internet. Networked systems on the Internet offer a low threshold for attacks and a high potential for damage.

This analysis focuses on the systems from charging station manufacturers and backend applications to manage charging stations. This sub-field was selected because of the large number of service providers attempting to establish themselves in the market. In a highly competitive environment, security is often a lower priority than market share and the implementation of new features. In addition, less attention was paid to IT security in the electrical installation sector and operational technology (OT) industry in the past, which has resulted in a shortage of specialists today.

Several standards and protocols have already been established in Switzerland and Europe to enable communication between manufacturers. For example, the OCPP (Open Charge Point Protocol) is used for the interaction between charging station and centralized backends. The way these interactions are implemented in practice was examined and reviewed from a cybersecurity perspective in this analysis.

Software which simulates the OCPP communication of a charging station was used for the tests. No charging stations were provided by the operators and none were procured by the NTC. No tests requiring physical access to a charging station were carried out. Attacks that require physical access often have a lower damage potential because they cannot be scaled with little effort.

A list of the systems which were tested during the analysis can be found below.

- Publicly accessible systems of around 50 different charging station manufacturers
- 7 mobile apps from manufacturers of charging stations and backend providers
- 4 firmware images of charging stations (11 in total, 4 of which were unencrypted)
- Applications from 23 organizations providing backends for charging stations

The following areas and aspects were NOT investigated in this analysis:

- Connection between the electric vehicle and the charging station
- Impact on the power grid: No tests were performed on systems which interact directly with the power grid
- Billing procedures between charging stations and charging station management systems

The tests carried out are intended to provide an initial overview of the security situation in the field of public charging infrastructure for electric mobility. Going in depth and investigating individual targets in detail was deliberately avoided. Therefore, mostly easily detectable vulnerabilities were identified. It must also be mentioned that it was not possible to procure dedicated hardware at a reasonable cost and in a reasonable time frame.

Furthermore, it must be stated that the affected organizations did not issue an audit. As a result, only limited tests could be carried out and care had to be taken not to cause any unintentional damage.

2.2 Scope of the Analysis in Detail

Figure 3 shows a schematic overview of the various stakeholders in the charging infrastructure. The diagram provides information about the areas investigated in this analysis.

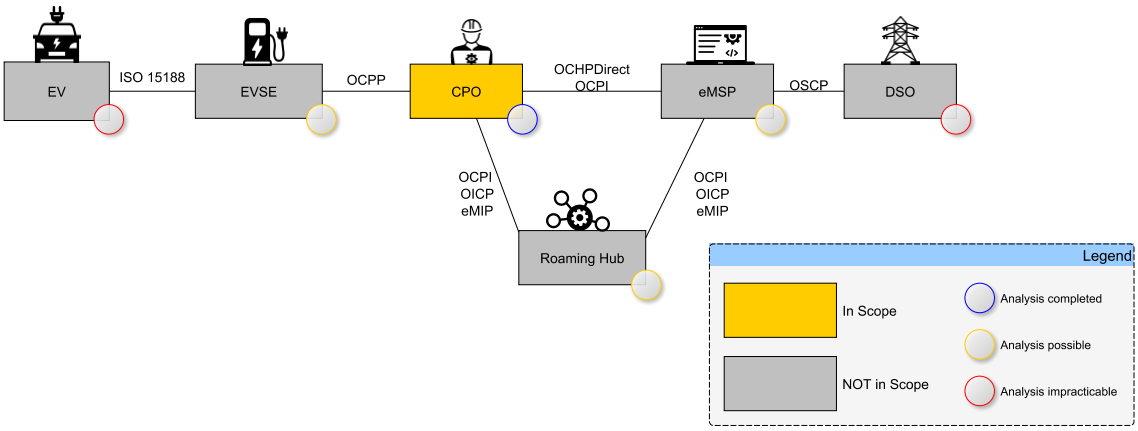

Figure 3: Charging infrastructure overview

The following list defines and explains the most important terms used in this report. Background information which gives a reason for the inclusion or exclusion of an area is also provided.

Electric Vehicle (EV)
The electric vehicle is generally connected to a charging station (electric vehicle supply equipment - EVSE) by means of a cable. There are various cable and connector types. The Type 2 cable for AC charging (generally slow charging) and the CCS cable for DC charging (generally fast charging) are the most common in Switzerland. In addition to power, the charging cable also transmits data. The vehicle communicates with the charging station, for example, to start or stop the charging process or to reduce the power if the battery can no longer absorb all the energy. Attacks using this means of communication have been demonstrated in the past (e.g. Brokenwire for CCS [3]). However, these types of attacks were not the subject of this review, as they require close physical proximity to the charging station, making large-scale attacks infeasible.

Electric Vehicle Supply Equipment (EVSE)
The charging station provides energy to charge electric vehicles. Charging stations are generally installed and operated by charge point operators (CPO). The charging stations are connected via the Internet to the CPO's centralized backend, called the Charging Station Management System (CSMS or CPMS), to ensure that the operator can manage them in a centralized manner. In Switzerland (and Europe in general), the Open Charge Point Protocol (OCPP) has become the standard for manufacturer-independent communication between the charging station and the CPO. The charging stations often communicate with the CPO via the cellular network. This requires the CSMS to be accessible via the Internet, making it vulnerable to cyberattacks. This communication channel was a particular focus of the examination, as a large part of the public charging infrastructure can be controlled, and thus potentially be paralyzed, by these few central systems. Furthermore, this part of the infrastructure is less visible than, for example, the payment apps and is therefore likely to be tested less thoroughly.

Charge Point Operator (CPO)
The charging station operators install and operate the charging stations and are generally not involved in billing of charging processes. They work either directly with an e-mobility service provider (eMSP) or with roaming hubs. Some CPOs also take on the role of the eMSP, operating both the charging stations and providing payment options for the end customers. Communication with the roaming hub or eMSP generally takes place via private connections (e.g. VPN, IP allowlisting etc.), so it was not possible to review this infrastructure as part of these tests. Several discussions with various companies were held in this regard, but unfortunately without success.

E-Mobility Service Provider (eMSP)
E-mobility service providers offer end users access to the public charging infrastructure, typically via apps and RFID customer cards. Ideally, the end users simply have to set up an account with an eMSP, enter their payment information and can then charge at most charging points, regardless of who actually operates the charging point. Due to direct interaction with the end user, the platforms operated by the eMSP, generally apps, are visible and accessible via the Internet. Accordingly, they are exposed to cyberattacks. Although these systems are rewarding targets for cyber criminals, they were not the focus of this review. The main reason for this is that while successful attacks can be extremely unpleasant for the individuals affected, be it the end users or operators, the attacks do not represent a significant threat to our society. For example, if an attacker manages to charge at a third party's expense by exploiting a vulnerability in an app. This is primarily a problem for the operators, not for Swiss society. It was therefore decided not to use any of the NTC's public funds for this purpose. It is the responsibility of the operators to operate a secure system and protect themselves against misuse.

Roaming Hub
A roaming hub acts as a link between the CPO and the eMSP, managing charging processes outside a user's own eMSP. A roaming hub works in the background and is not noticeable to the end user. It ensures that customers can charge at as many charging stations as possible using their RFID customer card or app. This process is also known as roaming. Since the roaming hubs do not interact directly with the end customer, but rather only with CPOs and eMSPs via private connections, there are very few areas that can be attacked via the Internet. Accordingly, almost no tests were carried out in this area.

3 Appendices

The Appendix provides an overview of the findings in Section 3.1, the detailed findings in Section 3.2, and the test cases which were examined for this analysis in Section 3.3.

3.1 List of Findings

All findings are listed below and grouped into one of three categories: high priority findings, medium priority findings, low priority findings. The findings have been anonymized and summarized according to the type of vulnerability. All findings are discussed in detail in Section 3.2.

High Priority (H)

Findings in this category are serious vulnerabilities and should be analyzed and addressed immediately. Attackers may exploit the vulnerabilities directly and cause severe damage.

Findings in this category may affect many or all users of the system. The vulnerabilities may be easily exploitable with sufficient privileges and are rather easy to detect. The vulnerabilities may be exploitable via the public Internet or by physically accessing a system. These vulnerabilities pose a realistic threat from amateurs and should be fixed immediately.

Medium Priority (M)

Findings in this category should be analyzed and corrected in the medium term. Attackers may be able to exploit the vulnerabilities and cause moderate damage.

Findings in this category affect a few to many users of a system. The vulnerabilities may be more difficult to exploit and it might require a more complex process to discover them. The vulnerabilities can be exploited via the Internet or by means of physical access to a system. The vulnerabilities therefore represent a realistic threat from sophisticated attackers and should be addressed as soon as possible.

Low Priority (L)

Findings in this category should be analyzed in the midterm and checked for rectification. Attackers may not be able to cause any immediate damage, but they can at least gain an advantage.

Findings in this category affect a small number of users or do not have any immediate impact on user data. These vulnerabilities are more difficult to exploit, have low potential to cause damage or require extensive permissions. Exploiting these vulnerabilities may require knowledge of the internal infrastructure or in-depth access to the systems. These vulnerabilities can be understood as “defense-in-depth” controls that would improve the overall hardening of the system.

3.2 Findings in Detail

This section documents all findings. The findings from different manufacturers are summarized depending on the type of the vulnerability. All findings listed have been reported to those concerned and, if possible, rectified.

This report does not disclose detailed description of the vulnerabilities, as the manufacturers were able to fully rectify them, and each of them assured the NTC, that the possibility of data leakage of Swiss citizens could be excluded.

Vulnerabilities that cannot be fixed by the manufacturer itself because the corrections have to be applied in various locations using a patch for example, will be published via a separate future information channel of the NTC and / or via CVE.

Section 3.2.1 (Page 12 onwards) describes the findings affecting operators of OCPP backends, and hence the systems CPOs and eMSPs. Section 3.2.2 from Page 23 onwards describes the findings from the examination of charging station manufacturers. Section 3.2.3 (Page 29 onwards) describes general findings in the charging infrastructure architecture and the industry in general.

3.2.1 Backend Systems

This section describes findings identified in the backend systems of CPOs and eMSPs.

Finding NTCF-191 M (Insufficient authentication for charging station backends):
Several providers use unencrypted and insecure mechanisms to authenticate charging stations. FB01 [20231012]

Background

Authentication in OCPP systems is intended to verify the identity of charging stations and backends before they communicate with each other. This prevents unauthorized access to the charging system and ensures the security of the transactions and data transmission.

Two types of authentications are described in the OCPP standard (1.6 and 2.0). HTTP BASIC authentication with username and password and certificate-based authentication [9]. In the case of authentication with HTTP BASIC, it should be noted that the credentials are only base64 encoded. Encoding must not be confused with encryption. The former can be readily converted back into plain text, hence it does not offer any security.

Several providers do not check authentication at all or use their own mechanism. For example, when logging in to a charging station, a customer ID needs to be entered as the only means of identification.

Distribution: 3 platforms

Preconditions

Attackers must be able to read the communication between the charging station and the backend. This can occur, for example, when a charging station is on the same WiFi network as the attackers. If the communication is encrypted, the attackers would also need to be able to break or bypass the encryption, which could be accomplished in the form of a man-in-the-middle attack.

Impact

The specific impact has not been provided in detail to keep the risk of potential damage as low as possible. Furthermore, the affected applications are different.

Recommendations

The backend and the charging stations should be authenticated using certificates, while communication should be securely encrypted and protected, for example by using TLS (Transport Layer Security). This ensures a secure and trustworthy connection between the two parties.

Finding NTCF-192 H (SQL injection): Various providers' web applications and OCPP endpoints were vulnerable to SQL injection. FB02 [20231012]

Background

Some web applications from various parties were affected by SQL injection vulnerabilities. It is therefore possible to insert a part of a database query into input fields, e.g. for the username, which is then inserted into the actual database query. As a result, usually all data in the database can be read out. Modifying the data may also be possible.

Distribution: 6 web applications

Preconditions

The vulnerable web applications are publicly accessible, hence no special preconditions are required.

Impact

The concrete impact on the vulnerable applications found has not been clarified in detail to keep the risk of potential damage as low as possible.

Usually, all content in the database can be read out. Depending on the content in the database, the data obtained may enable access to additional application functionalities. It may also be possible to change data in the database.

Recommendations

This problem often occurs if a database query is put together by merging static strings and user inputs (without sufficient validation or encoding). The following is recommended:

1. The use of *Prepared Statements* statements is recommended. It must be ensured that all parameters are implemented as such. The exact usage depends on the programming environment (language, framework and libraries). More details can be found at: `https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html#parameterized-query-examples`
2. User inputs should be limited to a minimal set of required input characters. Examples include: If a number is requested, it should be checked that a number in the expected range has been provided. In the case of names, it should be examined whether only permitted characters are provided.
3. User inputs should be encoded according to the database system used. Special functionalities are usually available in the framework or the program libraries. The following page provides more information: `https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html`

4. If one database query is vulnerable to SQL injection, all other queries should also be assessed to determine their security.

Finding NTCF-193 M (Cross-site scripting (XSS)): **For some providers, it was possible to insert malicious JavaScript code into the website, which was then executed.** FB03 [20231012]

Background

On a few charging station portals, users were able to insert their own content, in particular JavaScript code, via input. JavaScript code can be used to implement functionalities on websites. This content or these functionalities are then integrated into the actual page.

Distribution: 3 platforms

Preconditions

An account is required for all 3 web applications. This account can be created by attackers themselves via a registration page.

Impact

There are various conceivable scenarios for how the vulnerabilities could be exploited. One possibility would be to insert JavaScript code to steal an administrator's session cookie. An attacker could then use the session to exploit all the rights that an administrator has, which could significantly disrupt the operation of the charging stations.

Recommendations

The following recommendations help to prevent XSS vulnerabilities:

- Validate user inputs and limit them to the required minimum (character set, length etc.)
- User inputs should be encoded according to the context (e.g. HTML or JavaScript) when embedded in websites.
- Implement a Content Security Policy (CSP) which prohibits inline scripts from being executed.

Further recommendations can be found at: `https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html`

Finding NTCF-194 M (Improper authentication (auth bypass)): It was possible to bypass the login check of a provider's monitoring system FB04 [20231012]

Background

An OCPP monitoring website includes a check whether the website users were logged-in or not. If they are not, they are redirected to the login page.

However, the redirect also contained the whole website content which should only be available for logged-in users. Ignoring the redirect meant that the website could be used as if a user is logged in.

Distribution: 1 web application

Preconditions

Since the vendor's application is publicly accessible, no special preconditions are required.

Impact

Protected areas of the web application could be accessed. This meant that data theft was potentially also possible.

Recommendations

The implementation of the login check should be modified. It should be ensured that the application does not process user inputs or output confidential data if the login check fails.

Finding NTCF-195 H (Misconfiguration: Internal functionalities publicly accessible): Internal functionalities were publicly accessible FB05

Internal [20231012]

Background

Misconfigurations were found in several web applications which could allow attackers to use internal functions, e.g. SOAP-API or access to the cloud storage of the web application.

Distribution: 2 web applications

Preconditions

Only access to the web application is required. No credentials are required, or the necessary credentials are known default ones.

Impact

Potentially sensitive data could be read out, and it may also be possible to change or completely replace the web application. Writing to external data storage was also possible due to the misconfiguration.

Recommendations

In the case of web applications, it should be clarified whether each of the resources and functionalities are necessary and who needs access to them. Accordingly, the permissions should be set correctly, or the functionalities should be removed or blocked in general. It should also be ensured that strong passwords are used for all accounts.

Finding NTCF-196 H (Information Disclosure: Sensitive data in publicly accessible files): **Backup files and internal application files that were publicly available disclosed details about the system.** FB06 [20231012]

Background

Files (e.g. backup files) containing source code, passwords or other potentially sensitive data were accessible on multiple systems. These files are not required on the productive system for the actual functionality to work.

Distribution: 2 web applications

Preconditions

Only access to the web application is required.

Impact

The information could make it easier to find vulnerabilities. Access to the systems concerned with far-reaching consequences may be possible with the passwords disclosed.

Recommendations

It is recommended that functionalities and files that are not required on the productive systems are removed and to ensure that no files of this kind are included in the development process.

Finding NTCF-197 H (Information Disclosure: Development tools accessible): Activated developer tools in productive systems could be used to steal sensitive data. FB07 [20231012]

Background

Some vendors were found to have applications with debugging and development tools enabled. These tools help in the implementation of applications, for example by displaying all valid routes or configurations of a system.

Distribution: 6 web applications

Preconditions

Only access to the web application is required.

Impact

The developer tools may disclose information about the program flow or allow potentially far-reaching changes to the web application.

Recommendations

Developer tools should be particularly well protected in a similar way to the access of the administrator.

If the framework used allows, it should be ensured that the application is compiled and distributed in production mode.

Finding NTCF-198 H (Information Disclosure: Credentials in public source code): **Credentials were exposed on a public coding platform.** FB08 [20231012]

Background

An employee's source code was publicly accessible on a coding platform on the Internet. This code contained a potentially serious vulnerability in the form of sensitive information such as passwords.

Distribution: 1 service provider

Preconditions

Only access to the source code is required. The coding platform is publicly accessible and the project could be viewed without registration.

Impact

An attacker is able to log into other systems (e.g. administration console) unnoticed using another person's credentials.

Recommendations

It is recommended that passwords are removed from the source code before it is published. This check can also be automated. In addition, access credentials that have already been published should be invalidated and replaced. It is also important to check for additional credentials that may have been published at an earlier point in time.

It is generally recommended that all system users are only given the permissions necessary, and that multi-factor authentication is used on all systems during the login process.

Finding NTCF-199 H (Use of outdated software): An application with known vulnerabilities was not updated and was therefore an easy target for attackers. FB08 [20231012]

Background

Using obsolete software presents significant security risks, as obsolete programs often contain known vulnerabilities, making them more prone to attacks.

Distribution: 1 web application

Preconditions

The system is publicly accessible and there are already automated methods for exploiting the vulnerability.

Impact

It was potentially possible to use the known vulnerability to execute arbitrary code on the system.

Recommendations

A system update is recommended in which the software and all relevant components are updated to the latest versions.

It is also recommended keeping an inventory of all the software used and their respective versions. This allows one to quickly and potentially automatically determine which updates are required. This can also help to install updates across the whole company.

3.2.2 Charging Stations

Findings which concern the charging station manufacturers are recorded in this section.

Finding NTCF-200 L (Unprotected data on RFID cards): **RFID customer cards for identifying and authorizing users are not protected and can be copied.** FS01 [20231012]

Background

RFID cards are often used at charging stations to identify and authorize users. To start the charging process electric vehicle owners, place their RFID card next to the reader of the charging station. The reader then checks the card's customer ID and starts the charging process.

Previous reports like the one by Mathias Dalheimer show that RFID cards can be copied easily and the customer ID can be guessed in a short time [1]. The NTC verified and can confirm these findings.

Evidence

RFID cards from three charging infrastructure providers were randomly tested. All the customer cards could be read in just a few seconds using a Flipper Zero (portable multi-tool for wireless communication). The data read can then be copied to writable RFID cards or directly emulated as a card with the Flipper. The emulated cards are accepted at public charging stations without issue.

Preconditions

To copy and read an RFID card, it must be within a few centimeters of a reader.

Impact

It is possible to steal electricity on behalf of other customers, which is then billed to them.

Recommendations

It is recommended that unencrypted data on the cards is protected using PKI-based encryption. The standard *VDE-AR-E 2532-100* provides a detailed example of how this can be implemented [14].

An alternative would be to enable payment by credit card or via Android or iOS apps. Of course, there it is equally important to consider security. The communication should be encrypted and

protected against manipulation. Both the backend and the user must also be unequivocally authenticated.

Finding NTCF-201 H (Use of outdated OCPP standards): **Outdated versions of OCPP are used in many charging stations. A charging station's specifications often does not state with sufficient clarity which security features have been implemented.** FS02 [20231012]

Background

In the first versions, the OCPP standard was specified without any particular security features [6]. Only the encryption profiles for the data transfer were specified. Many missing security features have been added in the latest version `2.0.1` [8] and ported for the older version `1.6` in the form of a security whitepaper [7].

Examples of security features which were added retrospectively can be seen in Finding NTCF 202 and Finding NTCF 203.

Evidence

The NTC has randomly checked the datasheets and specifications of several charging stations. It was found that only `OCPP 1.6` or `OCPP 2.0.1` are listed as supported standards. In the case of `OCPP 1.6`, it is unclear whether the security features of the security whitepaper are also supported.

Impact

Security features which are present in the latest versions of OCPP are potentially missing in charging stations using `OCPP 1.6`. It is therefore unclear whether a secure update is possible, or an audit log is kept.

Recommendations

Charging station manufacturers should implement the missing security features and clearly state these in the specifications.

Finding NTCF-202 L (Insecure firmware update): **In the old versions of OCPP, no mechanism is described to ensure the firmware authenticity and integrity for firmware updates.** FS03 [20231012]

Background

In the OCPP protocol there is a message from the backend to the charging station which instructs the charging station to perform a firmware upgrade [6]. In this process, the charging station is sent a link from which the firmware is downloaded and installed.

If the charging station does not check the integrity of the update, attackers could potentially spread modified firmware to charging stations.

Evidence

In the first version of the `OCPP 1.6` standard, there was no mention of a mechanism for checking the authenticity and integrity of the firmware [6]. Section 8 states that signing of the firmware is recommended. However, this is not explained in more detail.

Preconditions

Attackers need to communicate with the charging station, which is using `OCPP 1.6` using WebSocket or SOAP without implementing the recommendations of the security whitepaper. Furthermore, they need to be able to impersonate a backend. Communication between the charging station and the backend takes places via the Internet and typically via the cellular network, which makes man-in-the-middle attacks more difficult.

Impact

Any firmware can be installed on the charging station.

Recommendations

The recommendations of the *OCPP 1.6 Security Whitepaper (3rd edition)* [7] or `OCPP 2.0.1` (without support of older insecure versions) should be implemented. The firmware should therefore be signed by the manufacturer, and the signature verified by the charging station prior to the installation.

Finding NTCF-203 L (Missing audit logs): **The original version of the OCPP 1.6 standard does not define which events are to be logged by a charging station and how the log data is to be transmitted.** FS03 [20231012]

Background

The original `OCPP 1.6` specification does not provide any information about an event log. There is therefore no guarantee that a log with security-relevant or other events will be available if necessary. This can make the search for errors or the detection and analysis of attacks more difficult or even impossible.

The specification only describes the possibility of retrieving diagnostic data from the back-end. However, there are no requirements specified in terms of the type and format of diagnosis data (this freedom is mentioned explicitly). Therefore, a charging station manufacturer is free to record event logs or diagnosis data and to make it available.

Evidence

In the first version of the `OCPP 1.6` standard, there is no mention of a mechanism for logging security-relevant events [6].

Preconditions

Implementation of the charging station according to the original `OCPP 1.6` specifications without further functionalities.

Impact

Security-relevant events are not logged and cannot be recorded in the backend. Analysis and alerting are therefore not easily possible.

Recommendations

Logging of security-relevant events as described in OCPP 1.6 Security Whitepaper (3rd edition), section 3 should be implemented.

Finding NTCF-204 L (Unencrypted firmware): Several charging station vendors allow unencrypted firmware to be downloaded. FS05 [20231012]

Background

The entire underlying operating system and the logic of a charging station constitute the charging station's firmware. Many manufacturers make their charging stations' firmware available on their websites or customer portals. Some firmware is not encrypted, and attackers can analyze it for vulnerabilities without a key.

Distribution 4 firmware files from various manufacturers

Preconditions

The firmware files are publicly accessible on the Internet and can be analyzed without decryption.

Impact

Since the firmware files can be analyzed without decryption, it is easier for attackers to search for vulnerabilities in depth. Furthermore, it is potentially possible to modify the firmware and install it on third-party charging stations via an update (see Finding NTCF 202).

The NTC has not investigated the unencrypted firmware files in detail.

Recommendations

It is recommended to encrypt the firmware such that it can only be decrypted by the charging station.

3.2.3 Conceptual Findings

Conceptual and industry-wide findings are described in this section.

Finding NTCF-205 M (Handling of multiple WebSocket connections): **The OCPP standard (1.6 and 2.0) does not specify what is expected to happen if there are multiple simultaneous WebSocket connections between a charging station and an OCPP backend. This could result in power theft or a charging station DoS.** FA01 [20231012]

Background

A study from Saiflow describes how different implementations of charging station management systems can be exploited to steal power from a charging station or take it offline by means of a denial of service attack [12].

This article explains in detail how this works: `https://www.saiflow.com/blog/how-mishandling-of-websockets-can-cause-dos-and-energy-theft`.

Distribution: 1 service provider

Evidence

The NTC has verified Saiflow's study for the Swiss market. With at least one provider, it is possible to disable the charging stations of an OCPP backend in principle.

For verification purposes, the messages of a charging station were imitated using a simulator[1]. This simulator was linked to an OCPP backend by entering the provider's OCPP URL and a fictitious charging station ID.

If a second connection with the same connection data is established in a separate browser window, the original WebSocket connection no longer receives any updates from the backend. Instead, all answers are sent to the second connection. Figure 4 shows this using *Heartbeat* messages.

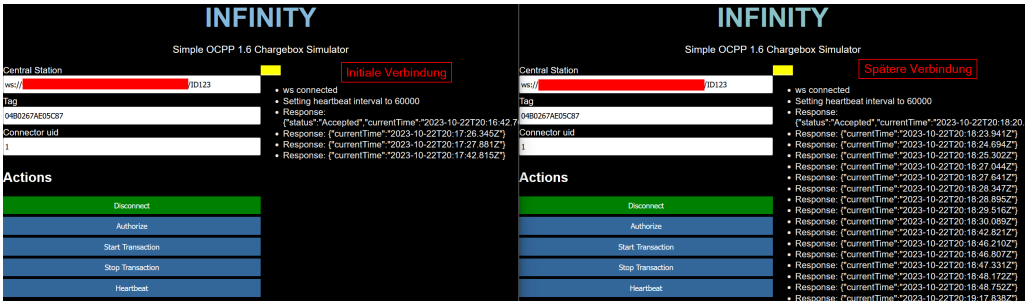

Figure 4: Simulator setup with two simultaneous connections

[1] https://github.com/victormunoz/OCPP-1.6-Chargebox-Simulator?tab=readme-ov-file

Preconditions

To block a charging station that can normally be accessed via the public Internet, the customer's OCPP-URL[2] and the charging station's serial number[3] are required.

Impact

Charging stations can potentially be disabled via the Internet.

Since this attack requires knowledge of difficult to guess customer IDs and the IDs of the target charging stations, the risk of this attack can be considered relatively low.

Recommendations

It is recommended that communication between the charging station and backend is established via a secure, private connection. Furthermore, backend connection attempts can be restricted geographically, i.e. blocking connections from outside Switzerland in order to reduce the risk.

In `OCPP 2.0.1`, authentication of the charging station to the backend is required [8], making this attack scenario significantly more difficult.

Further recommendations can be found at `https://www.saiflow.com/blog/how-mishandling-of-websockets-can-cause-dos-and-energy-theft/#How-CSMS-providers-can-mitigate-this-attack?`.

[2] The customer identification number is a 16-digit hex string, in other words there are 16^{16} possible combinations.
[3] There is no standard for charging station serial numbers. These can be determined by the manufacturer itself.

Finding NTCF-206 L (Point of contact not defined or difficult to reach): **There is no point of contact for security related issues at the majority of the affected parties, or the notifications are ignored.** FA02 [20231012]

Background

The NTC has reported vulnerabilities which were found in this analysis to the responsible parties. In this process, it was noticed that many organizations do not have a process how vulnerabilities can be reported.

Evidence

A dedicated point of contact which accepts reports concerning vulnerabilities could only be found at four organizations.

At many of the affected parties, emails and phone calls, which were made to general points of contact [4] were deliberately ignored or were forgotten. This is not a technical problem, but rather due to the lack of a defined process and the lack of awareness among support employees.

Impact

Vulnerabilities may result in violations of data protection provisions and the loss of customers, as trust among customers is compromised. The vulnerabilities could potentially serve as an entry point for additional attacks.

Ignoring security notifications reduces the likelihood that ethical hackers will report future vulnerabilities to the parties concerned.

Recommendations

It is recommended that a process for dealing with vulnerabilities is defined and enforced for the entire organization.

To make the reporting of vulnerabilities easier, it is recommended that a `security.txt` is included in the systems and kept up to date. This file includes relevant background information and up-to-date contact details. Further details on this can be found here: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html.

[4] For example, contact forms on the homepage, the hotline for the headquarters or via email to info@organization.net

3.3 Testcases

This section presents all test cases which were examined during the security analysis. Findings that arise from a particular test case are linked under the brief description of that case. If no finding is linked, no relevant vulnerability was found during the analysis. If a test case only applies to a subset of the components, the relevant components are explicitly listed.

3.3.1 Network Communication

The tests listed below show which tests were performed for the charging station management systems.

TC 1 Encrypted data transmission
Is network traffic transmitted in an encrypted way?
Risk: If the network traffic is not transmitted in encrypted form, the attacker can easily read or manipulate the communication content.
Findings: 191

TC 2 Encrypted data transmission with secure protocols
Are secure encryption protocols used for the encryption?
Risk: If the network traffic is transmitted using insecure protocols, this makes it easier for attackers to read or manipulate the communication content.

3.3.2 Charging Station Firmware

The test cases which were performed for the charging station firmware are listed below.

TC 3 Firmware encrypted
Is the firmware encrypted?
Risk: Firmware which is not encrypted can be directly analyzed by attackers. Since the entire operating system can be viewed, there is a large attack surface.
Findings: 204

TC 4 Credentials or access keys readable
Can credentials or access keys be found in the charging station firmware?
Risk: Access details which can be read out from the firmware allow attackers to access the relevant services.

TC 5 API endpoints
Can endpoints which are not used in a platform's web application be found in the firmware?
Risk: Additional API endpoints increase the attack surface of a platform.

3.3.3 Mobile Apps

Below is a list of checks used for mobile apps.

TC 6 API endpoints
Are API endpoints used in the app which are not used in a platform's web application?
Risk: Additional API endpoints increase the attack surface of a platform.

TC 7 Credentials readable
Does the mobile app contain hardcoded credentials or access keys?
Risk: Access details that can be read from compiled mobile apps can potentially allow attackers to use external services in the name of the mobile app.

3.3.4 Web Applications

The following test cases were used to evaluate web applications and web APIs.

TC 8 SQL injection
Is it possible to put malicious SQL commands in user inputs to access or manipulate databases? This was tested by sending apostrophes in form fields to the web application. Depending on the server's response to the input, an SQL injection vulnerability could be inferred with a high probability.
Risk: Disclosure of sensitive data, unauthorized access to the database and potential data manipulation.
Findings: 192

TC 9 Cross-site scripting (XSS)
Are attackers able to insert malicious JavaScript code in websites which is then executed?
Risk: Using XSS, arbitrary JavaScript code can be executed using XSS with the permissions of website visitors. Among other things, this can be used to steal user data, to impair the integrity of websites and to take over user sessions.
Findings: 193

TC 10 Login details in the source code
Can credentials or access keys be found in the source code of applications or systems? This examination was primarily performed manually or using tools such as TruffleHog.
Risk: Exposed credentials can be used to obtain unauthorized access to systems. Customer data leakage poses an additional risk.
Findings: 198

TC 11 Publicly available configuration files
Are there configuration files which can be accessed via the Internet? A list with common file names and tools such as dirsearch were used for this test.
Risk: Configuration files may contain login details for the database or services from third-party providers.
Findings: 196

TC 12 Publicly available backup files
Are there backup files which can be accessed via the Internet? A list with common file names and tools such as dirsearch were used for this test.
Risk: Backup files may contain login details for the database or services from third-party providers.
Findings: 196

TC 13 Active developer tools on the web application
Many frameworks for developing web applications offer tools for management and troubleshooting during development. Are attackers able to access these tools without any authentication?
Risk: Using the developer tools, it is potentially possible to read confidential file content, such as login details in configuration files.
Findings: 197

TC 14 Adding a charging station to a backend without authentication
Are attackers able to add a charging station without having the required credentials for the backend?
Risk: There is the possibility that fictional charging stations, which cannot be distinguished from real charging stations, can be added to the backend.
Findings: 191

References

[1] M. Dalheimer. Schwarzladen: Ladekarten manipulieren leicht gemacht. https://gonium.net/post/2017-10-26-schwarzladen/, Oct. 2017.

[2] Federal Department of Finance FDF. Security.txt - Include your security contact on your website. https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html, Jan. 2023.

[3] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic. Brokenwire : Wireless disruption of CCS electric vehicle charging, 2022.

[4] NCSC. Vulnerability disclosure management. https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/infos-it-spezialisten/Vulnerability_Disclosure_Management-Leitfaden_V1-0-EN.pdf.download.pdf, Oct. 2022.

[5] NTC. NTC Vulnerability Disclosure Policy (VDP). https://www.ntc.swiss/hubfs/NTC_Vulnerability_Disclosure_Policy.pdf, Aug. 2023.

[6] Open Charge Alliance. OCPP 1.6. https://www.openchargealliance.org/protocols/ocpp-16/, Sept. 2017.

[7] Open Charge Alliance. Improved security for OCPP 1.6-J. https://www.openchargealliance.org/protocols/ocpp-16/, Feb. 2022.

[8] Open Charge Alliance. OCPP 2.0.1 part 2 edition 2. https://www.openchargealliance.org/news/download-now-ocpp-201-part-2-edition-2/, Dec. 2022.

[9] Open Charge Alliance. Home - Open Charge Alliance. https://www.openchargealliance.org/, Oct. 2023.

[10] OWASP. OWASP Top 10-2017 (en). https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf, 2017.

[11] OWASP. OWASP Top 10:2021. https://owasp.org/Top10/, 2021.

[12] L. R. Saposnik. How Mishandling of WebSockets Can Cause DoS and Energy Theft, Feb. 2023.

[13] Swiss eMobility. Statistiken - Swiss eMobility. https://www.swiss-emobility.ch/de/Aktuell/Statistiken/, Sept. 2023.

[14] VDE VERLAG. VDE-AR-E 2532-100 Anwendungsregel:2021-07 - Standards. https://www.vde-verlag.de/standards/0500205/vde-ar-e-2532-100-anwendungsregel-2021-07.html, July 2021.