

Sicherheitsanalyse der Schweizer Ladeinfrastruktur für Elektromobilität

Eine technische Begutachtung

v1.0 / 15.11.2023

15. November 2023, 08:00

Document ID	NTC-20231115-1-de
Subject	Sicherheitsanalyse der Schweizer Ladeinfrastruktur für Elektromobilität
Version	v1.0 / 15.11.2023
Date	15. November 2023, 08:00
Classification	Öffentlich
Authors	Patrik Fabian, Dilip Many, Raphael M. Reischuk, Fabio Zuber
Responsible	Tobias Castagna

Inhaltsübersicht

1	Management Summary	2
1.1	Ausgangslage und Hintergrund	2
1.2	Zusammenfassende Einschätzung	3
1.3	Allgemeine Empfehlungen	5
1.4	Rahmenbedingungen	6
2	Umfang und Einschränkungen der Sicherheitsanalyse	7
2.1	Umfang der Analyse im Überblick	7
2.2	Umfang der Analyse im Detail	8
3	Anhänge	11
3.1	Befundliste	11
3.2	Befunde im Detail	13
3.2.1	Backend Systeme	13
3.2.2	Ladestationen	24
3.2.3	Konzeptionelle Befunde	30
3.3	Testfälle	33
3.3.1	Netzwerk Kommunikation	33
3.3.2	Firmware von Ladestationen	33
3.3.3	Mobile Apps	34
3.3.4	Webapplikationen	34

Änderungen

Version	Datum	Änderungen
1.0	2023-11-15, 08:00	Initiales Dokument

1 Management Summary

1.1 Ausgangslage und Hintergrund

Die Zahl der Elektrofahrzeuge auf Schweizer Strassen wächst rasant und eine Trendwende ist nicht in Sicht. Viele Fahrzeughersteller haben angekündigt, in naher Zukunft keine Fahrzeuge mit Verbrennungsmotoren mehr zu produzieren, auch weil diese in vielen Ländern in wenigen Jahren keine Strassenzulassung mehr erhalten dürften. Damit diese Wende im Strassenverkehr möglich wird, braucht es eine tragfähige Ladeinfrastruktur. Diese befindet sich in der Schweiz, in Europa und in vielen anderen Weltregionen derzeit im Aufbau.

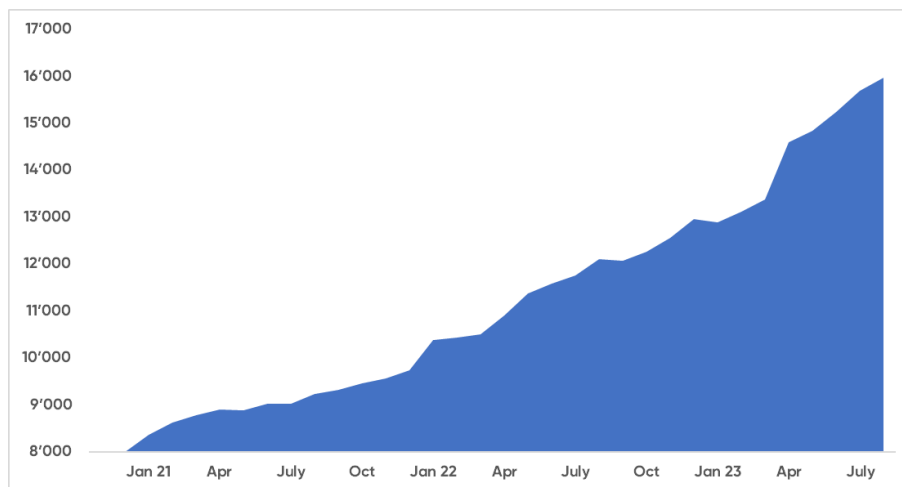


Abbildung 1: Anzahl Ladestationen der Schweiz. Quelle: Swiss eMobility: [13]

Es gibt eine Reihe von Faktoren, welche die öffentliche Ladeinfrastruktur besonders anfällig für Cyber-Angriffe machen. Im Vergleich zur herkömmlichen Tankstelleninfrastruktur ist die Ladeinfrastruktur wesentlich digitaler und vernetzter. Die Ladepunkte sind Computer, die mit dem Internet verbunden sind. Sie können über Apps gesteuert werden und sowohl die Abrechnung, als auch die Wartung erfolgen über zentrale Server der Betreiber. Durch die starke Vernetzung sind grossflächige Angriffe auf eine Vielzahl von Ladestationen und das Schweizer Stromnetz denkbar. Eine physische Nähe zur Ladestation ist für einen erfolgreichen Angriff nicht erforderlich.

Im Unterschied zur klassischen Energie-Infrastruktur ist die Technologie vergleichsweise neu und wird kontinuierlich weiterentwickelt. Es handelt sich also nicht um eine erprobte Technologie, die allgemein bekannt und vielfach überprüft ist. Die treibenden Kräfte in diesem Bereich sind eine Vielzahl von innovativen Start-ups, die in den letzten Jahren entstanden sind. Diese haben naturgemäss einen klaren Fokus auf eine möglichst schnelle Markteinführung und eine hohe Marktdurchdringung. Cybersicherheit steht dabei eher im Weg und hat oft wenig Priorität. Es wurde angenommen und die Resultate bestätigen es, dass deren Produkte und vernetzten Infrastrukturen heute zu wenig auf Verwundbarkeiten überprüft werden.

Das Nationale Testinstitut für Cybersicherheit NTC testet genau jene gesellschaftlich relevanten

Produkte und vernetzten Infrastrukturen, die gegenwärtig zu wenig getestet werden. Die Tests werden aus Eigeninitiative und mit Ressourcen des NTCs im Interesse der Schweizer Gesellschaft durchgeführt. Mit diesem Bericht werden die Ergebnisse dieser Überprüfung der Öffentlichkeit zugänglich gemacht.

Die Überprüfung konzentriert sich auf Risiken, die einen wesentlichen Einfluss auf die Sicherheit der Schweizer Gesellschaft haben. Beispiele dafür sind Schwachstellen, die es Angreifern erlauben, einen Grossteil der Ladeinfrastruktur für mehrere Tage oder Wochen ausser Betrieb zu setzen oder einen grossflächigen Stromausfall zu verursachen. Schwachstellen, die keine signifikanten Auswirkungen auf unsere Gesellschaft haben, stehen derzeit nicht im Fokus. Ein Beispiel wäre eine Schwachstelle, die es Angreifern erlaubt, auf fremde Kosten zu laden. Dies ist zwar für den einzelnen Betroffenen unangenehm, stellt aber keine Bedrohung für die Schweizer Gesellschaft dar.

Es ist den Autoren ein Anliegen, explizit darauf hinzuweisen, dass die Ergebnisse dieses Berichtes nicht dazu dienen sollen, die Elektromobilität zu schwächen. Im Gegenteil: Ziel ist es, in dieser frühen Ausbauphase auf mögliche Schwachstellen hinzuweisen, damit diese möglichst früh behoben werden können und eine robuste und leistungsfähige Ladeinfrastruktur für die Schweiz aufgebaut und betrieben werden kann.

1.2 Zusammenfassende Einschätzung

Ein Hauptrisiko liegt in der Verwendung des weit verbreiteten OCPP-Protokolls in der veralteten Version 1.6 durch einen Grossteil der Branche. OCPP steht für Open Charge Point Protocol und ist ein herstellerunabhängiges Kommunikationsprotokoll zur Verwaltung, Abrechnung und Überwachung von Ladestationen. Seit einigen Jahren steht die Protokollversion 2.0 bereit, die um wichtige Sicherheitsmerkmale erweitert wurde. De-facto-Standard ist jedoch die OCPP-Version 1.6 aus dem Jahr 2015, bei der wichtige Sicherheitsmerkmale gänzlich fehlen oder optional sind. So ist die Kommunikation zwischen Ladestation und Backend meist unverschlüsselt, die Authentifizierung der Ladestation gegenüber dem Backend unzureichend, keine Möglichkeiten für Monitoring oder Logging vorgeschrieben und der Updatemechanismus für die Firmware der Ladestationen ist als unsicher einzustufen.

OCPP 1.6 OPEN CHARGE POINT PROTOCOL	OCPP 2.0.1 OPEN CHARGE POINT PROTOCOL
<ul style="list-style-type: none">OCPP 1.5SOAP and JSONSmart Charging support for load balancing and use of charge profiles(Local) list management supportAdditional statusMessage sending requests such as CP time or status at the CP	<ul style="list-style-type: none">OCPP 1.6 plus added functionalitiesDevice ManagementImproved Transaction handlingAdded SecurityAdded Smart Charging functionalitiesSupport for ISO15118Display and messaging supportadditional improvements requested by the EV charging community

Abbildung 2: Vergleich der OCPP Versionen. Quelle: Open Charge Alliance [9]

Abgesehen von den oben beschriebenen Risiken im Zusammenhang mit OCPP, die einen Grossteil der Branche betreffen, wurde eine Vielzahl von Schwachstellen identifiziert, die einzelne Hersteller und Produkte betreffen. Die meisten dieser Verwundbarkeiten wurden in Backend-Systemen und nicht in den Ladestationen selbst identifiziert, da sich die Überprüfung auf erstere konzentrierte. Schwachstellen in Backend-Systemen wurden als kritischer eingestuft, da sie besser skalierbar sind und ein Angreifer mit weniger Aufwand eine grosse Anzahl von Verbrauchern aus der Ferne angreifen kann.

In den meisten Fällen handelt es sich um leicht erkennbare und ausnutzbare Verwundbarkeiten, die bereits früh durch automatisierte Tests identifiziert werden können. Dies deutet darauf hin, dass die Systeme nicht ausreichend auf Schwachstellen getestet werden. Am häufigsten wurden Systeme identifiziert, die entweder überhaupt nicht aus dem Internet erreichbar sein sollten oder die aufgrund einer Fehlkonfiguration mehr Informationen preisgeben als nötig. Beispielsweise wurden mehrere ungeschützte Konfigurationsdateien identifiziert, die Zugangsdaten und andere sensible Informationen enthielten. Andere Verwundbarkeiten sind auf veraltete Software zurückzuführen, was auf ein unzureichendes Patch-Management schliessen lässt.

Überraschend häufig wurden SQL Injection Schwachstellen identifiziert. Dies ist eine kritische Verwundbarkeitsklasse, die in der Vergangenheit weit verbreitet war, aber in den letzten Jahren dank moderner Entwicklungsframeworks und der Sensibilisierung der Entwickler seltener geworden ist. In den OWASP Top 10 von 2017 lagen Injection Schwachstellen noch auf Platz 1 [10]. Seit 2021 ist diese Verwundbarkeitsklasse auf Platz 3 abgerutscht, und das obwohl die weit verbreiteten Cross-Site-Scripting (XSS)-Angriffe neu mit eingerechnet werden [11]. Dies könnte darauf hindeuten, dass sich bestimmte gute Programmierpraktiken in der Branche der Ladeinfrastruktur noch nicht ausreichend durchgesetzt haben.

Insgesamt wurden Verwundbarkeiten an rund 30 Hersteller und Betreiber gemeldet. Erfreulicherweise wurden diese in der Regel innerhalb weniger Stunden oder Tage behoben. Als schwierig und zeitaufwändig erwies sich hingegen die Erreichbarkeit der betroffenen Organisationen. Während die verantwortlichen Organisationen in den meisten Fällen leicht ausfindig gemacht werden können, ist es deutlich schwieriger, die verantwortlichen Personen innerhalb der Organisationen zu identifizieren und zu erreichen. Eine Vulnerability Disclosure Policy, wie sie auch vom NCSC empfohlen wird [4], würde die Meldung von Verwundbarkeiten deutlich vereinfachen und beschleunigen, wurde aber leider von keinem der kontaktierten Unternehmen umgesetzt.

Weitere Details zu den identifizierten Risiken sind in [Abschnitt 3.2](#) ab [Seite 13](#) aufgeführt.

1.3 Allgemeine Empfehlungen

Aus den Ergebnissen dieser Überprüfung lassen sich folgende allgemeingültigen Empfehlungen für die Branche ableiten:

- Die aktuellste Version des OCPP-Protokolls sollte unterstützt und verwendet werden.
 - **OCPP 2.0.1 als Standard:** Alle neuen Ladestationen und OCPP-Backends sollen lediglich OCPP Version 2.0.1 oder neuer verwenden.
 - **Deprecation von OCPP 1.6:** Die Open Charge Alliance, die den OCPP-Standard definiert, sollte alte und unsichere Versionen des Protokolls als *deprecated* kennzeichnen und von ihrer Verwendung abraten.
- Sichere Programmierpraktiken sollten eingesetzt werden, um typische Sicherheitslücken wie SQL Injection und Cross-Site Scripting (XSS) zu vermeiden.
 - **Awareness (Sicherheitsbewusstsein):** Sensibilisierung der Entwickler für Sicherheitsrisiken während der Konzeption, der Entwicklung und des Betriebs.
 - **Einsatz moderner Frameworks:** Moderne Frameworks bieten oftmals bereits eingebaute Methoden zur sicheren Umsetzung einer Funktion.
 - **Code Reviews:** Regelmässige Überprüfung des Quellcodes auf korrekte Funktionalität und Sicherheit.
 - **Datenvvalidierung:** Implementierung umfassender Eingabeprüfungen und Validierungsmechanismen, um sicherzustellen, dass Benutzereingaben sicher verarbeitet werden.
- Die Angriffsfläche der Systeme sollte durch Härtungsmassnahmen reduziert werden.
 - **Sicherer Umgang mit Zugangsdaten:** Zugangsdaten sollten weder im Quellcode, noch in öffentlich zugänglichen Konfigurationsdateien auffindbar sein.
 - **Deaktivieren von Entwicklungsfunktionen:** Werkzeuge zur Fehlersuche sollten in produktiven Systemen deaktiviert oder eingeschränkt werden.
 - **Regelmässiges Einspielen von Security Patches:** Das zeitnahe Einspielen von Security Patches ist ein entscheidender Schritt, um potenzielle Sicherheitslücken zu schliessen und die Widerstandsfähigkeit eines Systems gegenüber Bedrohungen zu stärken.
- Die Erreichbarkeit für die Meldung von Sicherheitslücken durch ethische Hacker sollte erleichtert werden.
 - **security.txt einrichten:** Kontaktdaten für Sicherheitsmeldungen auf dem System zur

- Verfügung stellen. Das NCSC hat dazu ein Merkblatt veröffentlicht [2].
- **Vulnerability Disclosure Policy:** Richtlinie, die von Organisationen erstellt wird, um den Prozess der Meldung von Sicherheitslücken zu regeln. Das NCSC hat dafür ein Leitfaden für Unternehmen und Organisationen erstellt [4].
 - **Bug Bounty Programm aufsetzen:** Erhöht den Anreiz für ethische Hacker nach Sicherheitslücken zu suchen und diese verantwortungsvoll zu melden.
 - Beim Start des Ladevorgangs mit RFID-Karten sollte ein Verfahren verwendet werden, das auf asymmetrischer Kryptographie basiert und somit das Kopieren der Karten erschwert
 - **Verfahren auf Basis asymmetrischer Kryptographie:** Statt wie bisher nur die UID der RFID-Karte auszulesen, sollte auf ein Verfahren auf Basis asymmetrischer Kryptographie umgestellt werden. Die VDE-Anwendungsregel *VDE-AR-E-2532-100* [14] wird bereits von einigen Herstellern unterstützt und könnte eine Lösungsmöglichkeit darstellen.

Die Details über die detektierten Sicherheitslücken und die dazugehörigen Massnahmenempfehlungen wurden den betroffenen Organisationen im Rahmen des Responsible Disclosure Prozesses [5] vertraulich mitgeteilt. Eine anonymisierte Liste der Befunde ist im Anhang auf Seite 11 zu finden.

1.4 Rahmenbedingungen

Die Überprüfung wurde auf Initiative des NTCs durchgeführt. Das NTC hat die für die Überprüfung erforderlichen Ressourcen zur Verfügung gestellt und die Ziele, den Umfang und die Rahmenbedingungen festgelegt. Die betroffenen Hersteller und Betreiber hatten keinen Einfluss auf die Überprüfung. Es gibt keinen externen Auftraggeber.

Die Überprüfung fand zwischen Mai und August 2023 statt und wurde hauptsächlich von einem Kernteam von drei Testexperten des NTCs durchgeführt. Insgesamt wurden rund 90 Personentage aufgewendet für Recherche, Analyse, Test, Dokumentation und die Benachrichtigung und Beratung der rund 30 betroffenen Organisationen.

Es wurden nur Produkte und vernetzte Infrastrukturen getestet, die über das Internet erreichbar oder anderweitig öffentlich zugänglich sind. Es wurden keine Tests in internen Netzwerken oder nicht öffentlich zugänglichen Systemen der Hersteller und Betreiber durchgeführt.

Weitere Details bezüglich Umfang und Einschränkungen sind in [Abschnitt 2](#) ab [Seite 7](#) aufgeführt.

2 Umfang und Einschränkungen der Sicherheitsanalyse

In diesem Abschnitt wird der Umfang der durchgeführten Sicherheitsanalyse beschrieben. Dabei wird auch auf die selbst auferlegten sowie die technischen und ressourcenbedingten Einschränkungen eingegangen. Es folgt eine Übersicht über die wichtigsten Punkte, gefolgt von einer detaillierten Erläuterung.

2.1 Umfang der Analyse im Überblick

Das Nationale Testinstitut für Cybersicherheit NTC hat im Rahmen dieser Analyse die Sicherheitslage der Ladeinfrastruktur für Elektromobilität untersucht. Dabei wurde auf die Infrastruktur fokussiert, welche aus dem Internet erreichbar ist. Vernetzte Systeme im Internet bieten eine tiefe Schwelle für Angriffe und ein grosses Schadenspotenzial.

In dieser Analyse wurde auf die Systeme von Ladestation-Herstellern und Backend-Applikationen zum Verwalten von Ladestationen fokussiert. Dieser Teilbereich wurde ausgewählt, da hier eine grosse Anzahl an Leistungserbringern versuchen, sich auf dem Markt zu etablieren. Im starken Konkurrenzkampf kommt es oft vor, dass die Sicherheit tiefer priorisiert wird als Marktanteile und das Implementieren neuer Funktionen. Zudem wurden im Elektroinstallationsbereich und der Operational Technology (OT) Branche in der Vergangenheit weniger auf die IT-Sicherheit geachtet, was heute zu einem Mangel an Fachpersonen führt.

In der Schweiz und in Europa haben sich bereits einige Standards und Protokolle etabliert, um eine herstellerübergreifende Kommunikation zu ermöglichen. So wird OCPP (Open Charge Point Protocol) für die Interaktion zwischen Ladestation und zentralen Backends genutzt. In dieser Analyse wurde die praktische Umsetzung dieser Interaktionen unter die Lupe genommen und aus Sicht der Cybersicherheit überprüft.

Für die Tests wurde Software eingesetzt, welche die OCPP-Kommunikation einer Ladestation simuliert. Es wurden keine Ladestationen von den Betreibern zur Verfügung gestellt und auch keine vom NTC beschafft. Weitere Tests, welche physischen Zugriff zu einer Ladestation benötigten, wurden vom NTC nicht durchgeführt. Angriffe, welche physischen Zugriff benötigen, haben oft ein geringeres Schadenspotenzial, da sie nicht mit geringem Aufwand skaliert werden können.

Es folgt eine Liste der Systeme, welche im Rahmen der Untersuchung getestet wurden.

- Öffentliche Systeme von rund 50 verschiedenen Herstellern von Ladestationen
- 7 Mobile Apps von Herstellern von Ladestationen und Backendanbietern
- 4 Firmwares von Ladestationen (11 Total, 4 davon nicht verschlüsselt)
- Applikationen von 23 Organisationen, welche Backends für Ladestationen anbieten

Folgende Bereiche und Aspekte wurden in dieser Analyse nicht untersucht:

- Verbindung zwischen Elektrofahrzeug und Ladestation
- Auswirkungen auf das Stromnetz: Es wurden keine Systeme getestet, die direkt mit dem Stromnetz interagieren.
- Abrechnungsverfahren zwischen Ladestationen und Charging Station Management Systemen

Die durchgeführten Tests sollen einen ersten Überblick über die Sicherheitslage im Bereich der öffentlichen Ladeinfrastruktur für Elektromobilität geben. Es wurde bewusst darauf verzichtet, in die Tiefe zu gehen und einzelne Ziele im Detail zu untersuchen. Daher wurden eher leicht erkennbare Schwachstellen identifiziert. Darüber hinaus ist zu erwähnen, dass keine dedizierte Hardware mit vertretbarem Aufwand und in angemessener Zeit beschafft werden konnte.

Des Weiteren ist festzuhalten, dass kein Prüfauftrag der betroffenen Organisationen vorlag. Dies hatte zur Folge, dass nur begrenzte Tests durchgeführt werden konnten und darauf geachtet werden musste, keine unbeabsichtigten Schäden zu verursachen.

2.2 Umfang der Analyse im Detail

Die [Abbildung 3](#) zeigt eine schematische Übersicht über verschiedene Stakeholder bei der Ladeinfrastruktur. Das Diagramm gibt Aufschluss über die Teile, welche im Rahmen dieser Analyse untersucht wurden.

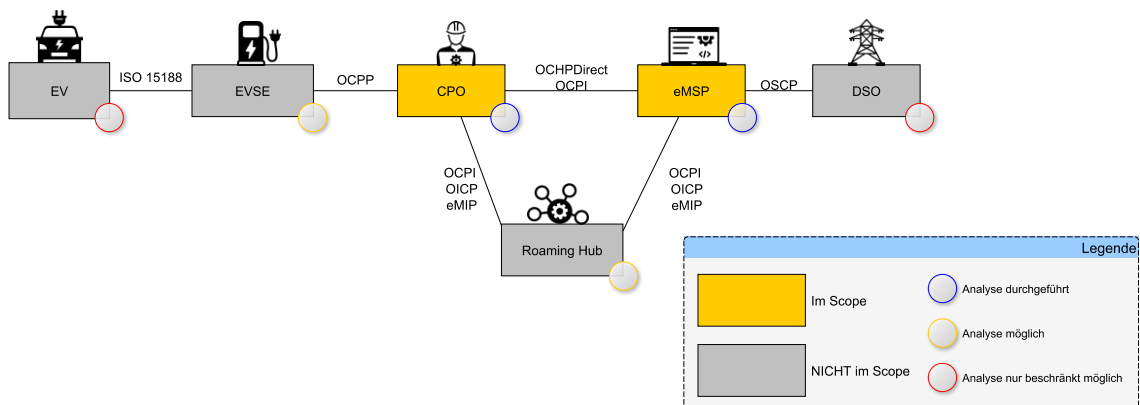


Abbildung 3: Ladeinfrastruktur Übersicht

Folgende Auflistung definiert und erläutert die wichtigsten in diesem Bericht verwendeten Begriffe. Ausserdem werden Hintergründe beschrieben, welche den Ein- oder Ausschluss eines Bereichs begründen.

Electric Vehicle (EV)

Das Elektrofahrzeug wird in der Regel mit einem Kabel an einer Ladestation (Electric Vehicle

Supply Equipment, EVSE) angeschlossen. Es gibt verschiedene Kabel- und Steckertypen, wobei in der Schweiz das Typ-2-Kabel für das AC-Laden (tendenziell langsames Laden) und das CCS-Kabel für das DC-Laden (tendenziell schnelles Laden) am weitesten verbreitet sind. Neben der Energie fließen auch Daten über das Ladekabel. Das Fahrzeug kommuniziert mit der Ladestation, um beispielsweise den Ladevorgang zu starten, zu stoppen oder die Leistung zu drosseln, wenn die Batterie nicht mehr die gesamte Energie aufnehmen kann. In der Vergangenheit wurden bereits Angriffe über diesen Kommunikationskanal demonstriert (z.B. Brokenwire für CCS [3]). Solche Angriffe waren jedoch nicht Gegenstand dieser Überprüfung, da sie eine unmittelbare physische Nähe zur Ladestation voraussetzen und somit keine grossflächigen Angriffe ermöglichen.

Electric Vehicle Supply Equipment (EVSE)

Die Ladestation liefert die Energie zum Laden von Elektrofahrzeugen. Ladestationen werden in der Regel von Charge Point Operators (CPO) installiert und betrieben. Damit die Ladestationen vom Betreiber zentral verwaltet werden können, sind sie über das Internet mit einem zentralen Backend des CPO verbunden, dem sogenannten Charging Station Management System (CSMS oder CPMS). Für die herstellerunabhängige Kommunikation zwischen Ladesäule und CPO hat sich in der Schweiz (und in Europa generell) das Open Charge Point Protocol OCPP etabliert. Die Ladestationen kommunizieren über das Mobilfunknetz mit dem CPO. Dazu muss das CSMS über das Internet erreichbar sein, was es anfällig für Cyber-Angriffe macht. Dieser Kommunikationskanal stand besonders im Fokus der Prüfung, da über diese wenigen zentralen Systeme ein Grossteil der öffentlichen Ladeinfrastruktur gesteuert und damit potenziell lahmgelegt werden kann. Darüber hinaus ist dieser Teil der Infrastruktur weniger sichtbar als z.B. die Bezahl-Apps und wird daher vermutlich weniger intensiv getestet.

Charge Point Operator (CPO)

Die Ladestation-Operatoren installieren und betreiben die Ladestationen und kümmern sich in der Regel nicht um die Abrechnung der Ladevorgänge. Dazu arbeiten sie entweder direkt mit e-Mobility Service Provider (eMSP) oder mit Roaming Hubs zusammen. Einige CPOs übernehmen auch die Rolle des eMSPs und betreiben gleichzeitig die Ladestationen und stellen die Zahlungsmöglichkeiten zur Verfügung, über die die Endkunden bezahlen können. Die Kommunikation mit dem Roaming Hub bzw. dem eMSP erfolgt in der Regel über private Verbindungen (z.B. VPN, IP Allowlisting etc.), so dass eine Überprüfung dieser Infrastruktur im Rahmen dieses Tests nicht möglich war. Es wurden diesbezüglich mehrere, leider erfolglose Gespräche mit verschiedenen Unternehmen in diesem Bereich geführt.

E-Mobility Service Provider (eMSP)

E-Mobility Service Provider bieten den Endnutzern Zugang zur öffentlichen Ladeinfrastruktur, typischerweise über Apps und RFID-Kundenkarten. Im Idealfall muss der Endnutzer nur ein Konto bei einem eMSP einrichten, seine Zahlungsinformationen hinterlegen und kann dann an den meisten Ladepunkten laden, unabhängig davon, wer den Ladepunkt tatsächlich betreibt. Durch die direkte Interaktion mit dem Endnutzer sind die von den eMSP betriebenen Plattformen, in der Regel Apps, gut sichtbar und über das Internet erreichbar. Dementsprechend sind sie Cyber-Angriffen ausgesetzt. Obwohl diese Systeme lohnende Ziele für Cyber-Kriminelle darstellen, standen sie nicht im Fokus der Überprüfung. Der Hauptgrund dafür ist, dass erfolgreiche Angriffe zwar für die einzelnen Betroffenen, seien es Endnutzer oder Betreiber, sehr unangenehm sein können, aber keine signifikante Bedrohung für unsere Gesellschaft darstellen. Wenn

es einem Angreifer beispielsweise gelingt, über eine Schwachstelle in einer App auf fremde Kosten zu laden, ist dies in erster Linie ein Problem für die Betreiber, nicht aber für die Schweizer Gesellschaft, weshalb entschieden wurde, dafür keine öffentlichen Mittel des NTC zu verwenden. Es liegt in der Verantwortung der Betreiber, ein sicheres System zu betreiben und sich vor Missbrauch zu schützen.

Roaming Hub

Ein Roaming Hub fungiert als Bindeglied zwischen CPO und eMSP und kümmert sich um die Vermittlung von Ladevorgängen ausserhalb des eigenen eMSPs. Ein Roaming Hub agiert im Hintergrund und ist für Endkunden nicht wahrnehmbar. Er sorgt dafür, dass Endkunden mit ihrer RFID-Ladekarte oder App an möglichst vielen Ladestation laden können (auch Roaming genannt). Da die Roaming Hubs nicht direkt mit dem Endkunden, sondern nur mit CPOs und eMSPs über private Verbindungen interagieren, ist die Angriffsfläche gegenüber dem Internet sehr gering. Dementsprechend wurden in diesem Bereich praktisch keine Tests durchgeführt.

3 Anhänge

Im Anhang finden sich die Befunde im Überblick in [Abschnitt 3.1](#), die detaillierten Befunde in [Abschnitt 3.2](#), sowie die Testfälle welche für diese Analyse überprüft wurden in [Abschnitt 3.3](#).

3.1 Befundliste

Im Folgenden werden alle Befunde aufgeführt und in einer von drei Kategorien gruppiert: Befunde hoher Priorität, Befunde mittlerer Priorität, Befunde niedriger Priorität. Die Befunde wurden anonymisiert und zusammengefasst nach Typ der Sicherheitslücke. Alle Befunde werden im Detail in [Abschnitt 3.2](#) behandelt.

Hohe Risiken (H)

Befunde in dieser Kategorie entsprechen schwerwiegenden Schwachstellen und sollten sofort analysiert und korrigiert werden. Angreifer können die Schwachstellen möglicherweise direkt ausnutzen und schweren Schaden anrichten.

NTCF-192 H	FB02	SQL Injection	15
NTCF-195 H	FB05	Fehlkonfiguration: Interne Funktionalitäten öffentlich zugänglich	19
NTCF-196 H	FB06	Information Disclosure: Sensitive Daten in öffentlich zugänglichen Dateien	20
NTCF-197 H	FB07	Information Disclosure: Entwicklungswerkzeuge erreichbar	21
NTCF-198 H	FB08	Information Disclosure: Zugangsdaten in öffentlichem Quellcode	22
NTCF-199 H	FB08	Einsatz veralteter Software	23
NTCF-201 H	FS02	Verwendung veralteter OCPP Standards	26

Die Befunde in dieser Kategorie können viele oder alle Benutzende des Systems betreffen. Die Schwachstellen können mit ausreichenden Berechtigungen leicht ausnutzbar sein und sind eher leicht zu erkennen. Die Schwachstellen können über das öffentliche Internet oder durch physischen Zugriff auf ein System ausnutzbar sein. Diese Schwachstellen stellen eine realistische Bedrohung durch Amateure dar und sollten baldmöglichst behoben werden.

Mittlere Risiken (M)

Befunde in dieser Kategorie sollten mittelfristig analysiert und korrigiert werden. Angreifer können die Schwachstellen möglicherweise ausnutzen und Schaden mittleren Ausmasses anrichten.

NTCF-191 M	FB01	Unzureichende Authentifizierung bei Ladestation-Backends	13
NTCF-193 M	FB03	Cross-Site Scripting (XSS)	17
NTCF-194 M	FB04	Improper Authentication (Auth Bypass)	18
NTCF-205 M	FA01	Handling von mehreren WebSocket Verbindungen	30

Befunde in dieser Kategorie betreffen wenige bis viele Benutzende des Systems. Die Schwachstellen sind möglicherweise schwieriger auszunutzen, und es kann aufwendiger sein, sie zu entdecken. Die Schwachstellen können über das Internet oder durch physischen Zugriff auf ein System ausnutzbar sein. Diese Schwachstellen stellen somit eine realistische Bedrohung durch fortgeschrittene Angreifer dar und sollten innerhalb kurzer Zeit behoben werden.

Geringe Risiken (L)

Befunde in dieser Kategorie sollten mittelfristig analysiert und auf Behebung überprüft werden. Angreifer können möglicherweise keinen unmittelbaren Schaden anrichten, aber sie können sich zumindest einen Vorteil verschaffen.

NTCF-200	L	FS01	Ungeschützte Daten auf RFID-Karten	24
NTCF-202	L	FS03	Unsicheres Firmwareupdate	27
NTCF-203	L	FS03	Fehlende Ereignisprotokolle (Audit Logs)	28
NTCF-204	L	FS05	Unverschlüsselte Firmware	29
NTCF-206	L	FA02	Kontaktstelle nicht definiert oder schwer erreichbar	32

Befunde in dieser Kategorie betreffen eine kleine Anzahl von Benutzenden oder haben keine unmittelbaren Auswirkungen auf Benutzerdaten. Die Schwachstellen sind eher kompliziert auszunutzen, haben ein geringes Schadenspotential oder erfordern umfangreiche Berechtigungen. Die Ausnutzung dieser Schwachstellen erfordert möglicherweise Kenntnisse der internen Infrastruktur oder einen tiefen Zugriff auf die Systeme. Diese Schwachstellen können als "Defense-in-Depth"-Kontrollen verstanden werden, die die Gesamthärtung des Systems verbessern würden.

3.2 Befunde im Detail

In diesem Abschnitt werden alle Befunde dokumentiert. Die Befunde verschiedener Hersteller werden je nach Art der Sicherheitslücke zusammengefasst. Alle aufgeführten Befunde wurden den betroffenen Stellen gemeldet und wenn möglich behoben.

In diesem Bericht wird auf eine detaillierte Offenlegung der Sicherheitslücken verzichtet, da die Lücken vollständig von Herstellern behoben werden konnten und dem NTC jeweils zugesichert werden konnte, dass ein Datenabfluss von Schweizer Betroffenen ausgeschlossen werden kann.

Sicherheitslücken, welche nicht selbstständig vom Hersteller korrigiert werden können, da sie beispielsweise via Patch an verschiedenen Orten verteilt werden müssen, werden über einen zukünftigen separaten Informationskanal des NTCs und / oder via CVE publiziert.

So beschreibt [Abschnitt 3.2.1 \(Seite 13 ff.\)](#) die Befunde, welche bei Betreibern von OCPP-Backends, also bei den Systemen von **CPOs** und **eMSPs** festgestellt wurden. [Abschnitt 3.2.2 \(Seite 24 ff.\)](#) beschreibt die Erkenntnisse, welche bei der Untersuchung von Herstellern von Ladestationen festgestellt wurden. Das Kapitel [Abschnitt 3.2.3 \(Seite 30 ff.\)](#) beschreibt allgemeine Befunde in der Architektur der Ladeinfrastruktur und der Branche im Gesamten.

3.2.1 Backend Systeme

Dieses Kapitel beschreibt Befunde, die in Backend Systemen von **CPOs** und **eMSPs** gefunden wurden.

Befund NTCF-191 **M** (Unzureichende Authentifizierung bei Ladestation-Backends): **Einige Anbieter verwenden unverschlüsselte und unsichere Mechanismen zur Authentifizierung von Ladestationen.** **FB01** [20231012]

Hintergrund

Die Authentifizierung in OCPP-Systemen dient dazu, die Identität von Ladestationen und Backends zu überprüfen, bevor sie miteinander kommunizieren. Dies verhindert unbefugten Zugriff auf das Ladesystem und gewährleistet die Sicherheit der Transaktionen und Datenübertragung.

Im OCPP Standard (1.6 und 2.0) werden zwei Arten von Authentifizierungen beschrieben. HTTP BASIC Authentifizierung via Benutzername und Passwort und eine zertifikatsbasierte Authentifizierung [7]. Bei einer Authentifizierung mittels HTTP BASIC gilt zu beachten, dass die Zugangsdaten lediglich base64 codiert werden. Eine Codierung kann direkt in den Klartext zurückgewandelt werden und ist keine Verschlüsselung. Sie bietet daher keinerlei Sicherheit.

Bei einigen Anbietern wird die Authentifizierung gar nicht oder durch einen eigenen Mechanismus überprüft. So muss bei der Anmeldung einer Ladestation zum Beispiel eine Kundennummer angegeben werden, welche als einziges Erkennungsmerkmal gilt.

Verbreitung: 3 Plattformen

Vorbedingungen

Angreifer müssen die Kommunikation zwischen der Ladestation und dem Backend mitlesen können. Dies kann zum Beispiel passieren, wenn sich eine Ladestation im gleichen W-LAN Netzwerk wie die Angreifer befinden. Falls die Kommunikation verschlüsselt ist, müssten die Angreifer ebenfalls in der Lage sein diese zu brechen oder zu umgehen. Dies wäre z.B. in Form einer Man-in-the-Middle Attacke umsetzbar.

Auswirkungen

Die konkreten Auswirkungen wurden nicht im Detail abgeklärt, um das Risiko eines möglichen Schadens minimal zu halten. Des Weiteren sind die betroffenen Applikationen unterschiedlich.

Empfehlungen

Die Authentifizierung des Backends und der Ladestation sollte mit Hilfe von Zertifikaten erfolgen, während die Kommunikation sicher verschlüsselt und geschützt sein sollte, beispielsweise durch die Verwendung von TLS (Transport Layer Security). Dies gewährleistet eine sichere und vertrauenswürdige Verbindung der beiden Parteien.

Befund NTCF-192 H (SQL Injection): Webapplikationen und OCPP-Endpunkte verschiedener Anbieter waren verwundbar auf SQL Injection. FB02 [20231012]

Hintergrund

Einige Webapplikationen diverser Akteure waren von SQL Injection Verwundbarkeiten betroffen. Daher ist es möglich in Eingabefeldern, z.B. für den Benutzernamen, einen Teil einer Datenbankabfrage einzufügen, welche dann in die eigentliche Abfrage eingefügt wird. Dadurch können meist alle Daten der Datenbank ausgelesen werden. Eine Modifikation der Daten kann unter Umständen auch möglich sein.

Verbreitung: 6 Webapplikationen

Vorbedingungen

Die verwundbaren Webapplikationen sind öffentlich zugänglich. Daher sind keine speziellen Vorbedingungen nötig.

Auswirkungen

Die Auswirkungen für die gefunden verwundbaren Applikationen wurden nicht im Detail abgeklärt, um das Risiko eines möglichen Schadens minimal zu halten.

Generell kann meist der gesamte Inhalt der Datenbank ausgelesen werden. Je nach dessen Inhalt können die gewonnenen Daten auch Zugriff auf weitere Funktionalitäten einer Applikation ermöglichen. Das Verändern der Daten in der Datenbank kann auch möglich sein.

Empfehlungen

Das Problem entsteht oft, wenn eine Datenbankabfrage durch Zusammenfügen von statischen Strings und Benutzereingaben (ohne genügende Validierung oder Codierung) konstruiert wird. Folgendes wird empfohlen:

1. Es wird empfohlen *Prepared Statements* zu verwenden. Dabei muss beachtet werden, dass sämtliche Parameter als solche erfasst werden. Die genaue Benutzung ist von der Programmierumgebung (Sprache, Framework und Bibliotheken) abhängig. Mehr Details finden sich unter: https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html#parameterized-query-examples
2. Benutzereingaben sollten auf ein minimales Set von benötigten Eingabezeichen beschränkt werden. Beispiele: Wenn eine Zahl abgefragt wird, sollte geprüft werden, ob eine Zahl im erwarteten Bereich angegeben wurde. Bei Namen ist zu prüfen, ob nur erlaubte Zeichen in der Eingabe vorkommen, etc.

3. Benutzereingaben sollten entsprechend dem benutzten Datenbanksystem codiert werden. Dazu sind meist spezielle Funktionalitäten im Framework oder den Programm-bibliotheken vorhanden. Mehr dazu ist auf der folgenden Seite zu finden: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
4. Wenn eine Datenbankabfrage verwundbar auf SQL Injection ist, sollten alle anderen Abfragen ebenfalls auf deren Sicherheit überprüft werden.

Befund NTCF-193 **M** (Cross-Site Scripting (XSS)): **Bei einigen Anbietern war es möglich, bösartigen JavaScript Code in der Webseite einzufügen, welcher ausgeführt wurde.** **FB03**

[20231012]

Hintergrund

Bei einigen wenigen Ladestation-Portalen ist es Benutzenden möglich via Eingabe eigene Inhalte, insbesondere JavaScript-Code, einzufügen. JavaScript-Code ist Code, welcher zur Umsetzung von Funktionalitäten auf Webseiten benutzt werden kann. Diese Inhalte resp. Funktionalitäten werden dann in die eigentliche Seite integriert.

Verbreitung: 3 Plattformen

Vorbedingungen

Bei allen 3 Applikationen wird ein Account für die Webapplikation benötigt, welcher über eine eigenständige Registrierung erstellt werden kann.

Auswirkungen

Es sind diverse Szenarien denkbar, wie die Lücken verwendet werden könnten. Eine Variante wäre es JavaScript-Code einzufügen, um das Sitzungscookie eines Administrators zu stehlen. Anschliessend könnte ein Angreifer die Sitzung benutzen, um sämtliche Möglichkeiten eines Administrators auszunutzen. Dies könnte den Betrieb der Ladesäulen wesentlich stören.

Empfehlungen

Die folgenden Empfehlungen helfen zur Verhinderung von XSS Verwundbarkeiten:

- Benutzereingaben validieren und auf das nötige Minimum (Zeichensatz, Länge, etc.) beschränken.
- Benutzereingaben sollen bei einer Einbettung in Webseiten entsprechend dem Kontext (z.B. HTML oder JavaScript) codiert werden.
- Content Security Policy (CSP) einrichten, welche das Ausführen von Inline-Skripten untersagt.

Weitere Empfehlungen sind zu finden unter: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Befund NTCF-194 **M** (Improper Authentication (Auth Bypass)): **Der Login-Check des Monitoring Systems eines Herstellers konnte übergangen werden.** **FB04** [20231012]

Hintergrund

Die Webseite eines Herstellers enthält eine Überprüfung, ob die Benutzenden der Webseite angemeldet sind. Falls dies nicht der Fall ist, werden sie auf die Anmeldeseite weitergeleitet.

Die Weiterleitung enthielt gleichzeitig aber den gesamten Webseiteninhalt, welcher nur für angemeldete Benutzende vorgesehen ist. Daher konnte durch das Ignorieren der Weiterleitung die Webseite auch ohne Anmeldung gleich wie mit einer Anmeldung benutzt werden.

Verbreitung: 1 Webapplikation

Vorbedingungen

Da die Applikation des Herstellers öffentlich zugänglich ist, werden keine besonderen Vorbedingungen benötigt.

Auswirkungen

Es war möglich geschützte Bereiche der Webapplikation zu erreichen. Somit ist ein Datendiebstahl potenziell auch möglich.

Empfehlungen

Die Implementierung der Login-Überprüfung soll angepasst werden. Dabei sollte darauf geachtet werden, dass die Applikation weder Benutzereingaben verarbeitet noch vertrauliche Daten ausgibt, wenn die Login-Überprüfung negativ ausfällt.

Befund NTCF-195 **H** (Fehlkonfiguration: Interne Funktionalitäten öffentlich zugänglich): **In-**
terne Funktionalitäten waren öffentlich zugänglich **FB05** [20231012]

Hintergrund

Bei einigen Webapplikationen wurden Fehlkonfigurationen gefunden, was es Angreifern erlauben könnte interne Funktionen, z.B. SOAP-API oder Cloudspeicher für die Webapplikation, zu benutzen.

Verbreitung: 2 Webapplikationen

Vorbedingungen

Es ist lediglich der Zugriff auf die Web-Applikation notwendig. Es sind keine Zugangsdaten notwendig oder es handelt sich um bekannte Standard-Zugangsdaten.

Auswirkungen

Dadurch können potenziell sensitive Daten ausgelesen und eventuell auch die Web-Applikation verändert oder komplett ersetzt werden. Durch die Fehlkonfiguration war das Schreiben auf externen Datenspeicher möglich.

Empfehlungen

Bei Webapplikationen sollte für alle Ressourcen und Funktionalitäten abgeklärt werden, ob diese notwendig sind und wer darauf Zugriff haben muss. Entsprechend sollten die Berechtigungen korrekt gesetzt oder die Funktionalitäten generell entfernt oder blockiert werden. Zudem sollte darauf geachtet werden, dass für alle Konten starke Passwörter verwendet werden.

Befund NTCF-196 **H** (Information Disclosure: Sensitive Daten in öffentlich zugänglichen Dateien): **Sicherungsdateien und interne Applikations-Dateien, welche öffentlich aufrufbar waren, gaben Details über das System preis.** **FB06** [20231012]

Hintergrund

Auf mehreren Systemen waren Dateien (z.B. Sicherungsdateien) aufrufbar, welche Quellcode, Passwörter oder andere potenziell sensitive Daten enthalten. Diese Dateien werden für die eigentliche Funktionalität nicht auf dem Produktivsystem benötigt.

Verbreitung: 2 Webapplikationen

Vorbedingungen



Es ist lediglich der Zugriff auf die Web-Applikation notwendig.

Auswirkungen

Die Informationen können das Auffinden von Sicherheitslücken erleichtern. Bei den preisgegebenen Passwörtern ist allenfalls ein Zugriff auf die betroffenen Systeme mit weiterreichenden Folgen möglich.

Empfehlungen

Es wird empfohlen, nicht benötigte Funktionalitäten und Dateien auf den Produktivsystemen zu entfernen und sicherzustellen, dass im Entwicklungsprozess keine solche Dateien einfließen.

Befund NTCF-197  (Information Disclosure: Entwicklungswerkzeuge erreichbar): **Aktivierte Entwicklerfunktionen in produktiven Systemen konnten genutzt werden, um sensitive Daten zu stehlen.**  [20231012]

Hintergrund

Bei einigen Anbietern wurden Applikationen gefunden, welche Debugging- und Entwicklungswerkzeuge aktiviert hatten. Diese Werkzeuge helfen beim Implementieren von Applikationen, indem sie zum Beispiel alle gültigen Routen oder Konfigurationen eines Systems anzeigen.

Verbreitung: 6 Webapplikationen

Vorbedingungen

Es ist lediglich der Zugriff auf die Web-Applikation notwendig.

Auswirkungen

Die Entwicklungswerkzeuge können Informationen über den Programmablauf preisgeben oder potenziell weitreichende Veränderungen an der Web-Applikation erlauben.

Empfehlungen

Entwicklungswerkzeuge sollten ähnlich wie Administratorenzugänge besonders abgesichert werden.

Falls das verwendete Framework dies erlaubt, sollte darauf geachtet werden, dass die Applikation im produktiven Modus kompiliert und verteilt wird.

Befund NTCF-198  (Information Disclosure: Zugangsdaten in öffentlichem Quellcode): **Zugangsdaten waren auf öffentlicher Coding-Plattform exponiert.**  [20231012]

Hintergrund

Der Quellcode eines Mitarbeitenden ist im Internet öffentlich einsehbar auf einer Coding-Plattform. Dieser Code beinhaltet eine potenziell schwerwiegende Sicherheitslücke, da sensible Informationen wie Passwörter im Code enthalten sind.

Verbreitung: 1 Dienstleister

Vorbedingungen

Es ist lediglich der Zugriff auf den Quellcode notwendig. Die Coding-Plattform ist öffentlich zugänglich und das Projekt war ohne Registrierung einsehbar.

Auswirkungen

Es ist einem Angreifer möglich, sich unauffällig mit den Zugangsdaten einer anderen Person bei weiteren Systemen (z.B. Administrationskonsole) anzumelden.

Empfehlungen

Es wird empfohlen, Passwörter aus dem Quellcode vor dessen Veröffentlichung zu entfernen. Dies kann allenfalls auch automatisiert erfolgen. Zudem sollten die bereits veröffentlichten Zugangsdaten für ungültig erklärt und ersetzt werden. Dabei ist auch zu prüfen, ob eventuell schon in der Vergangenheit weitere Zugangsdaten veröffentlicht wurden.

Generell wird empfohlen allen Benutzenden eines Systems nur die notwendigen Berechtigungen zu geben und auf allen Systemen mehrere Faktoren für die Anmeldung zu verwenden.

Befund NTCF-199 **H** (Einsatz veralteter Software): **Eine Applikation mit bekannten Sicherheitslücken wurde nicht aktualisiert und bot so ein einfaches Ziel für Angreifer.** **FB08** [20231012]

Hintergrund

Der Einsatz von veralteter Software bringt erhebliche Sicherheitsrisiken, da veraltete Programme oft bekannte Sicherheitslücken enthalten und daher für Angriffe anfälliger sind.

Verbreitung: 1 Webapplikation

Vorbedingungen

Das System ist öffentlich zugänglich und es existieren bereits automatisierte Methoden, um die Sicherheitslücke auszunutzen.

Auswirkungen

Mit Hilfe der bekannten Sicherheitslücke war es potenziell möglich beliebigen Code auf dem System auszuführen.

Empfehlungen

Es wird empfohlen, das System auf den neuesten Stand zu bringen, indem die Software und alle relevanten Komponenten auf die neusten Versionen aktualisiert werden.

Ausserdem wird empfohlen ein Inventar aller eingesetzter Software und deren Versionen zu führen, um einen Update-Bedarf schnell (eventuell automatisiert) feststellen zu können. Dies kann auch helfen die Updates flächendeckend einzuspielen.

3.2.2 Ladestationen

In diesem Kapitel werden Erkenntnisse, welche die Hersteller von Ladestationen betrafen, festgehalten.

Befund NTCF-200 L (Ungeschützte Daten auf RFID-Karten): **RFID-Kundenkarten für die Identifizierung und Autorisierung von Benutzenden sind nicht geschützt und können kopiert werden.** FS01 [20231012]

Hintergrund

Bei Ladestationen werden RFID-Karten oftmals zur Identifizierung und Autorisierung von Benutzenden verwendet. Elektrofahrzeug Fahrende halten ihre RFID-Karte an das Lesegerät der Ladestation, welche die Kundennummer der Karte überprüft und den Ladevorgang startet.

Vorgängige Berichte wie jener von Mathias Dalheimer zeigen, dass die RFID-Karte leicht kopiert werden kann und die Kundennummer in kurzer Zeit erraten werden kann [1]. Das NTC kann diese Befunde bestätigen.

Nachweis

Stichprobenartig wurden RFID-Karten von drei Ladeinfrastruktur-Anbietern getestet. Alle Kundenkarten konnten mit Hilfe eines Flipper Zero (Portables Multi-Tool für Drahtlos-Kommunikation) innerhalb von wenigen Sekunden ausgelesen werden. Die ausgelesenen Daten können anschliessend auf beschreibbare RFID-Karten kopiert werden oder direkt mit dem Flipper als Karte emuliert werden. Die emulierten Karten werden ohne Probleme an öffentlichen Ladestationen akzeptiert.

Vorbedingungen

Zum Kopieren und Auslesen einer RFID-Karte, muss sich jene innerhalb von ein paar Zentimeter zu einem Lesegerät befinden.

Auswirkungen

Es ist möglich im Namen von anderen Kunden Strom zu beziehen, welcher diesen dann verrechnet wird.

Empfehlungen

Es wird empfohlen, die unverschlüsselten Daten auf den Karten mit Hilfe von PKI-basierter Verschlüsselung zu schützen. Ein Beispiel wie dies im Detail umgesetzt werden kann, zeigt der Stan-

dard *VDE-AR-E 2532-100* [14].

Alternativ wäre es auch möglich die Bezahlung mit Kreditkarten oder via Android- oder iOS-Apps zu ermöglichen. Natürlich muss hierbei gleichermassen auf die Sicherheit geachtet werden. Die Kommunikation sollte verschlüsselt und vor Manipulation gesichert sein. Zudem müssen sowohl das Backend, als auch der Benutzer zweifelsfrei authentifiziert werden.

Befund NTCF-201 H (Verwendung veralteter OCPP Standards): Bei vielen Ladestationen werden veraltete Versionen von OCPP unterstützt. In der Spezifikation einer Ladestation wird oft nicht klar definiert, welche Sicherheitsmerkmale umgesetzt wurden. FS02 [20231012]

Hintergrund

Der OCPP Standard wurde in den ersten Versionen ohne besondere Sicherheitsfunktionen spezifiziert [6]. Einzig die Verschlüsselungs-Profile für die Datenübertragung werden vorgegeben. Viele fehlende Sicherheitsfunktionen wurden in der neusten Version 2.0.1 hinzugefügt [8] und in Form eines Security Whitepapers für die ältere Version 1.6 des Standards portiert [7].

Beispiele für Sicherheitsfunktionen, welche im Nachhinein hinzugefügt wurden, zeigen [Befund NTCF 202](#) und [Befund NTCF 203](#).

Nachweis

Das NTC hat Stichprobenartig die Datenblätter und Spezifikationen von einigen Ladestationen überprüft. Dabei ist aufgefallen, dass jeweils lediglich ocpp 1.6 oder ocpp 2.0.1 als unterstützte Standards aufgelistet werden. Im Falle von ocpp 1.6 ist jeweils unklar, ob die Sicherheitsfunktionen des Security Whitepapers ebenfalls unterstützt werden.

Auswirkungen

Sicherheitsfunktionen, die bei neuen Versionen von OCPP vorhanden sind, fehlen potenziell bei Ladestationen mit ocpp 1.6. Dadurch ist unklar, ob ein sicheres Update möglich ist oder ein Auditlog geführt wird.

Empfehlungen

Die Hersteller von Ladestationen sollen die fehlenden Sicherheitsfunktionen implementieren und jene klar in den Spezifikationen festhalten.

Befund NTCF-202 L (Unsicheres Firmwareupdate): In alten Versionen von OCPP wird bezüglich Firmware Aktualisierung kein Mechanismus beschrieben, um die Authentizität und Integrität der Firmware sicherzustellen. **FS03** [20231012]

Hintergrund

Im OCPP-Protokoll gibt es eine Nachricht vom Backend zur Ladestation, welche die Ladestation instruiert ein Firmware-Upgrade durchzuführen [6]. Dabei wird der Ladestation ein Link mitgeteilt, von wo sie ihr Update herunterladen und installieren soll.

Wenn die Ladestation die Integrität des Updates nicht prüft, können Angreifer potenziell modifizierte Firmware auf Ladestationen verteilen.

Nachweis

In der ersten Version des `ocpp 1.6` Standards wird kein Mechanismus zur Überprüfung der Authentizität und Integrität der Firmware erwähnt [6]. In Kapitel 8 wird erwähnt, dass die Signierung der Firmware empfohlen wird. Allerdings wird dies nicht genauer erläutert.

Vorbedingungen

Angreifer müssen mit der Ladestation, welche `ocpp 1.6` ohne Empfehlungen des Security Whitepapers einsetzt, über WebSocket oder SOAP kommunizieren und sich gegenüber dieser als Backend ausgeben können. Die Kommunikation zwischen der Ladestation und dem Backend läuft über das Internet und typischerweise über das Mobilfunknetz, was Man-in-the-Middle Angriffe erschwert.

Auswirkungen

Es ist möglich auf der Ladesäule beliebige Firmwares zu installieren.

Empfehlungen

Es sollten die Empfehlungen des *OCPP 1.6 Security Whitepaper (3rd edition)* [7] umgesetzt oder auf `ocpp 2.0.1` (ohne Unterstützung älterer unsicherer Versionen) umgestellt werden. Somit sollte die Firmware vom Hersteller signiert werden und die Signatur vor der Installation durch die Ladestation überprüft werden.

Befund NTCF-203 L (Fehlende Ereignisprotokolle (Audit Logs)): In der ursprünglichen Version des OCPP 1.6 Standards wird nicht definiert, welche Ereignisse durch eine Ladestation protokolliert werden sollen und wie Log Daten übermittelt werden sollen. FS03 [20231012]

Hintergrund

Die originale OCPP 1.6 Spezifikation macht keine Angaben zu einem Ereignisprotokoll. Daher ist es nicht gegeben, dass im Bedarfsfall ein Protokoll mit sicherheitsrelevanten oder anderen Ereignissen zur Verfügung steht. Dies kann die Suche nach Fehlern oder auch die Detektion und Analyse von Angriffen erschweren oder verunmöglichen.

Die Spezifikation beschreibt lediglich die Möglichkeit zum Abruf von Diagnosedaten durch das Backend. Wobei bezüglich Art und Format der Diagnosedaten keinerlei Vorgaben gemacht werden (diese Freiheit ist explizit erwähnt). Daher steht es einem Ladesäulen-Hersteller frei, Ereignisprotokolle oder Diagnosedaten zu erfassen und diese verfügbar zu machen.

Nachweis

In der ersten Version des OCPP 1.6 Standards wird kein Mechanismus zum Protokollieren von sicherheitsrelevanten Ereignissen erwähnt [6].

Vorbedingungen



Implementation der Ladestation nach der originalen OCPP 1.6 Spezifikationen ohne weitergehende Funktionalitäten.

Auswirkungen

Sicherheitsrelevante Ereignisse werden nicht protokolliert und können auch nicht im Backend erfasst werden. Daher ist auch eine Analyse und eine Alarmierung nicht ohne weiteres möglich.

Empfehlungen

Es sollte eine Protokollierung von sicherheitsrelevanten Ereignissen wie im [OCPP 1.6 Security Whitepaper \(3rd edition\)](#), Kapitel 3 beschrieben, implementiert werden.

Befund NTCF-204  (Unverschlüsselte Firmware): **Einige Hersteller von Ladestation erlauben es unverschlüsselte Firmwares herunterzuladen.**  [20231012]

Hintergrund

Das gesamte unterliegende Betriebssystem und die Logik einer Ladestation bilden die Firmware einer Ladestation. Viele Hersteller stellen die Firmware ihrer Ladestationen auf der Webseite oder in Kundenportalen zur Verfügung. Gewisse Firmwares sind nicht verschlüsselt und lassen sich ohne Entschlüsselung durch Angreifer auf Sicherheitslücken analysieren.

Verbreitung: 4 Firmwares verschiedener Hersteller

Vorbedingungen

Die Firmwares sind öffentlich im Internet zugänglich und können ohne Entschlüsselung analysiert werden.

Auswirkungen

Da die Firmwares ohne Entschlüsselung analysiert werden können, ist Angreifern eine detaillierte Suche nach Schwachstellen leichter möglich. Weiter ist es potenziell möglich, die Firmware zu modifizieren und auf fremde Ladestationen via Update einzuspielen (siehe [Befund NTCF 202](#)).

Das NTC hat die unverschlüsselten Firmwares nicht im Detail untersucht.

Empfehlungen

Es wird empfohlen, die Firmware so zu verschlüsseln, dass sie lediglich von der Ladestation entschlüsselt werden kann.

3.2.3 Konzeptionelle Befunde

Die konzeptionellen und branchenumfassenden Befunde werden in diesem Kapitel beschrieben.

Befund NTCF-205 M (Handling von mehreren WebSocket Verbindungen): Im OCPP Standard (1.6 und 2.0) ist nicht spezifiziert, was passieren soll, wenn mehrere gleichzeitige WebSocket-Verbindungen zwischen einer Ladestation und einem OCPP-Backend bestehen. Dies kann zu Stromdiebstahl oder einem DoS der Ladestation führen. FA01 [20231012]

Hintergrund

In einer Studie von Saiflow wird beschrieben, wie verschiedene Implementierungen von Charging Station Management Systemen ausgenutzt werden können, um Strom einer Ladestation zu stehlen oder sie mittels eines Denial-of-Service vom Netz zu nehmen [12].

Wie dies funktioniert wird in diesem Artikel ausführlich erklärt: <https://www.saiflow.com/blog/how-mishandling-of-websockets-can-cause-dos-and-energy-theft>

Verbreitung: 1 service provider

Nachweis

Das NTC hat die Studie von Saiflow für den Schweizer Markt verifiziert. Bei mindestens einem Anbieter ist es prinzipiell möglich die Ladestationen eines OCPP-Backends funktionsunfähig zu machen.

Für die Verifikation wurden die Nachrichten einer Ladestation mit Hilfe eines Simulators¹ imitiert. Dieser Simulator wurde mit einem OCPP-Backend gekoppelt, indem die OCPP-URL des Anbieters und eine fiktive ID einer Ladestation eingegeben wurden.

Wenn in einem separatem Browserfenster eine zweite Verbindung mit den gleichen Verbindungsdaten aufgebaut wird, erhält die ursprüngliche WebSocket Verbindung keine Updates mehr vom Backend. Stattdessen werden alle Antworten an die zweite Verbindung gesendet. Die Abbildung 4 zeigt dies anhand von *Heartbeat* Nachrichten.

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

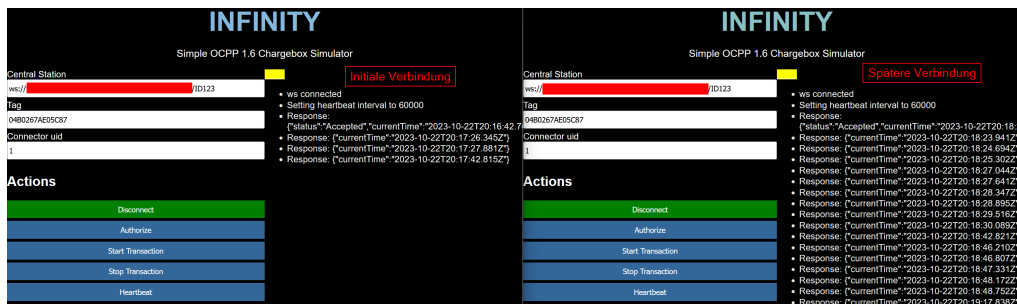


Abbildung 4: Simulator Aufbau mit zwei gleichzeitigen Verbindungen

Vorbedingungen

Um eine Ladestation, welche im Normalfall über das öffentliche Internet erreichbar ist, zu blockieren, wird die kundeneigene² OCPP-URL, sowie die Seriennummer³ der Ladestation benötigt.

Auswirkungen

Es ist potenziell möglich Ladestationen vom Internet aus funktionsunfähig zu machen.

Da für diesen Angriff schwer erratbare Kundennummern und die IDs der Ziel-Ladestationen bekannt sein müssen, ist das Risiko für diesen Angriff trotzdem als relativ gering einzustufen.

Empfehlungen

Es wird empfohlen, die Kommunikation der Ladestation mit dem Backend über eine gesicherte, private Verbindung herzustellen. Des Weiteren kann das Backend Verbindungsversuche geografisch einschränken, d.h. Verbindungen von ausserhalb der Schweiz zu blockieren, um das Risiko etwas zu reduzieren.

In `ocpp 2.0.1` wird eine Authentifizierung der Ladestation gegenüber dem Backend vorgeschrieben [8], was dieses Angriffsszenario deutlich erschwert.

Weitere Empfehlungen finden sich unter <https://www.saiflow.com/blog/how-mishandling-of-websockets-can-cause-dos-and-energy-theft/#How-CSMS-providers-can-mitigate-this-attack?>.

² Die Kunden-Identifikationsnummer ist ein 16-stelliger Hex String, sprich 16^{16} mögliche Kombinationen.

³ Für Seriennummern von Ladestationen gibt es keinen Standard. Diese kann vom Hersteller selbst bestimmt werden.

Befund NTCF-206 L (Kontaktstelle nicht definiert oder schwer erreichbar): **Bei vielen Betroffenen ist keine Kontaktstelle für Sicherheitsmeldungen definiert oder die Meldungen werden ignoriert.** FA02 [20231012]

Hintergrund

Sicherheitslücken, die in dieser Analyse gefunden wurden, sind durch das NTC bei den zuständigen Stellen gemeldet worden. Dabei ist aufgefallen, dass bei vielen Organisationen kein Prozess definiert ist, wie Sicherheitslücken gemeldet werden können.

Nachweis

Bei nur vier Organisationen konnte eine dedizierte Stelle gefunden werden, welche Meldungen zu Sicherheitslücken entgegennimmt.

Bei vielen Betroffenen wurden E-Mails und Telefonate, welche bei allgemeinen Stellen⁴ platziert wurden, bewusst ignoriert oder sind vergessen gegangen. Dies ist kein technisches Problem, sondern liegt am Fehlen eines definierten Prozesses und der Sensibilisierung von Support-Mitarbeitenden.

Auswirkungen

Schwachstellen können zu Datenschutzverletzungen und Kundenverlust führen, da das Vertrauen der Kunden erschüttert wird. Die Lücken können potenziell auch als Einfallstor für weitere Angriffe dienen.

Wenn Sicherheitsmeldungen nicht beachtet werden, sinkt die Chance, dass ethische Hacker zukünftige Lücken bei den Betroffenen melden.

Empfehlungen

Es wird empfohlen, einen Prozess für die Behandlung von Sicherheitslücken zu definieren und diesen für die gesamte Organisation geltend zu machen.

Um das Melden von Sicherheitslücken zu erleichtern, wird empfohlen ein `security.txt` auf den Systemen zu platzieren und aktuell zu halten. Dieses enthält relevante Hintergrundinformationen und aktuelle Kontaktdaten. Weitere Details dazu finden sich hier: <https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html>.

⁴ Zum Beispiel Kontaktformulare auf der Homepage, die Hotline des Hauptsitzes oder via E-Mail an `info@organisation.net`

3.3 Testfälle

In diesem Abschnitt werden alle Testfälle vorgestellt, die während der Sicherheitsanalyse betrachtet wurden. Befunde, die aus einem bestimmten Testfall hervorgehen, sind unter der Kurzbeschreibung des Testfalls verlinkt. Wenn kein Befund verlinkt ist, wurde im Zeitrahmen der Analyse keine relevante Schwachstelle gefunden. Wenn ein Testfall nur für eine Teilmenge der Komponenten gelten, werden die entsprechenden Komponenten explizit aufgeführt.

3.3.1 Netzwerk Kommunikation

Die nachfolgend aufgeführten Tests zeigen welche Überprüfungen für Charging Station Management Systeme durchgeführt wurden.

TF 1 Verschlüsselte Datenübertragung

Wird der Netzwerkverkehr verschlüsselt übertragen?

Risiko: Wird der Netzwerkverkehr nicht verschlüsselt übertragen, so ist es für Angreifer einfach möglich, den Inhalt der Kommunikation mitzulesen oder zu manipulieren.

Befunde: [191](#)

TF 2 Verschlüsselte Datenübertragung mit sicheren Protokollen

Wird die Verschlüsselung mit sicheren Verschlüsselungs-Protokollen durchgeführt?

Risiko: Wird der Netzwerkverkehr mit unsicheren Protokollen übertragen, erleichtert dies den Angreifern, den Inhalt der Kommunikation mitzulesen oder zu manipulieren.

3.3.2 Firmware von Ladestationen

Unten sind die Testfälle aufgeführt, welche für die Firmwares von Ladestationen durchgeführt wurden.

TF 3 Firmware verschlüsselt

Ist die Firmware verschlüsselt?

Risiko: Firmware welche nicht verschlüsselt ist, kann von Angreifern direkt analysiert werden. Da das gesamte Betriebssystem eingesehen werden kann, bietet sich eine grosse Angriffsfläche.

Befunde: [204](#)

TF 4 Zugangsdaten auslesbar

Finden sich Zugangsdaten in der Firmware von Ladestationen?

Risiko: Zugangsdaten, welche aus der Firmware gelesen werden können, erlauben Angreifern den Zugriff auf die entsprechenden Dienste.

TF 5 API-Endpunkte

Finden sich in der Firmware Endpunkte, welche in der Webapplikation einer Plattform nicht verwendet werden?

Risiko: Zusätzliche API Endpunkte erhöhen die Angriffsfläche einer Plattform.

3.3.3 Mobile Apps

Es folgt eine Liste mit den Überprüfungen, mit welchen Mobile Apps überprüft wurden.

TF 6 API Endpunkte

Werden in der App API Endpunkte genutzt, welche in der Webapplikation einer Plattform nicht verwendet werden?

Risiko: Zusätzliche API Endpunkte erhöhen die Angriffsfläche einer Plattform.

TF 7 Zugangsdaten auslesber

Finden sich in der Mobile App Zugangsdaten zu Backend Diensten?

Risiko: Zugangsdaten, welche aus kompilierten Mobile Apps gelesen werden können, erlauben es Angreifern potenziell externe Dienste im Namen der Mobile App zu nutzen.

3.3.4 Webapplikationen

Die folgenden Testfälle wurden genutzt um Webapplikationen zu evaluieren.

TF 8 SQL Injection

Ist es möglich schädliche SQL-Befehle in Benutzereingaben einzuschleusen, um auf Datenbanken zuzugreifen oder sie zu manipulieren? Konkret wurde dies überprüft, indem Hochkommas in Formularfeldern an die Webapplikation gesendet wurden. Je nach Antwort des Servers auf die Eingabe konnte bereits mit hoher Wahrscheinlichkeit auf eine SQL Injection Lücke geschlossen werden.

Risiko: Offenlegung von sensiblen Daten, unbefugter Zugriff auf die Datenbank und mögliche Datenmanipulation.

Befunde: 192

TF 9 Cross-site Scripting (XSS)

Ist es für Angreifer möglich böartigen JavaScript Code in Webseiten einzufügen, welcher ausgeführt wird?

Risiko: Mittels XSS kann arbiträrer JavaScript Code mit den Berechtigungen von Webseiten Besuchenden ausgeführt werden. Dies kann unter anderem zum Benutzerdaten Diebstahl, zur Beeinträchtigung der Integrität von Webseiten und zur Übernahme von Benutzersitzungen genutzt werden.

Befunde: 193

TF 10 Anmelddaten in Quellcode

Können sensible Zugangsdaten (z.B. Benutzername und Passwort) im Quellcode von Anwendungen oder Systemen gefunden werden? Diese Überprüfung wurde primär manuell oder mit Hilfe von Tools wie [TruffleHog](#) durchgeführt.

Risiko: Offenlegung von Zugangsdaten, die ausgenutzt werden könnten, um unbefugten Zugriff zu Systemen zu erhalten. Ein potenzieller Abfluss von Kundendaten ist ein weiteres Risiko.

Befunde: [198](#)

TF 11 Öffentlich exponierte Konfigurationsdateien

Gibt es Konfigurationsdateien, welche aus dem Internet aufgerufen werden können? Um dies zu testen wurde eine Liste mit gängigen Dateinamen und Tools wie [dirsearch](#) eingesetzt.

Risiko: In Konfigurationsdateien können Anmelddaten zur Datenbank oder Diensten von Drittanbietern gefunden werden.

Befunde: [196](#)

TF 12 Öffentlich exponierte Sicherungsdateien

Gibt es Sicherungsdateien, welche aus dem Internet aufgerufen werden können? Um dies zu testen wurde eine Liste mit gängigen Dateinamen und Tools wie [dirsearch](#) eingesetzt.

Risiko: In Sicherungsdateien können Anmelddaten zur Datenbank oder Diensten von Drittanbietern gefunden werden.

Befunde: [196](#)

TF 13 Aktive Entwicklerwerkzeuge auf der Webapplikation

Viele Frameworks für die Entwicklung von Webapplikationen bieten Werkzeuge zur Verwaltung und Fehlersuche während der Entwicklung. Ist es Angreifern möglich diese Werkzeuge ohne Authentifizierung aufzurufen?

Risiko: Mit Hilfe der Entwicklerwerkzeuge ist es potenziell möglich, vertrauliche Dateiinhalte wie z.B. Anmelddaten in Konfigurationsdateien auszulesen.

Befunde: [197](#)

TF 14 Ladestation ohne Authentifizierung zum Backend hinzufügen

Ist es Angreifern möglich, eine Ladestation hinzuzufügen, ohne Zugriffsdaten zum Backend zu haben?

Risiko: Es besteht die Möglichkeit, fiktive Ladestationen zum Backend hinzuzufügen, welche nicht unterscheidbar zu realen Ladestationen sind.

Befunde: [191](#)

Literatur

- [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.