ABL

Lauf, 04.01.2017

Stellungnahme zur Sicherheit unserer Ladesäulen (1/2)

Im Update „Chaos Computer Club hackt Ladesäulen“ des CCC und im Beitrag „Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit“ von Mathias Dalheimer zum 34. Chaos Communication Congress werden drei Thematiken angesprochen.

Die erste angesprochene Schwachstelle hat der CCC wie folgt beschrieben: *„Die meisten Ladestationen erlauben das Ändern der Konfiguration sowie Firmwareupdates über einen USB-Stick. Da der Updatemechanismus beispielsweise bei KEBA-Ladestationen unsicher ist, kann beliebiger Code in die Ladestation eingeschleust werden. Darüber könnten Angreifer beispielsweise alle Ladevorgänge gratis machen oder aber wiederum die Kartennummern ernten und so Ladekartenkunden schädigen.“*
Dies trifft auf Ladestationen von ABL nicht zu: Die USB-Schnittstellen sind bei Ladestationen von ABL nicht von außen erreichbar, ein Zugriff auf diese ermöglicht zudem kein Auslesen von gespeicherten Transaktionsdaten. Die Software des Kommunikationscontrollers in Ladestationen von ABL kann nur mit einer kryptographisch signierten Updatedatei aktualisiert werden.

Die zweite Schwachstelle, *vorhandene RFID - Karten kopieren, vervielfältigen und anschließend an einer unserer Ladestationen verwenden zu können*, ist grundsätzlich möglich. Dabei wird die Nutzer-ID der Ladekarte ausgelesen, anschließend vervielfältigt und kann so an einer Ladestation genutzt werden. Bei den von Backend-Betreibern ausgegebenen Ladekarten hat sich der eher unsichere Standard Mifare Classic durchgesetzt. Es gibt aber auch RFID-Karten wie ULTRALIGHT C und DESfire, die eine durch Verschlüsselung geschützte Datenübertragung unterstützen. Da unser RFID-Lesegerät auch für die Nutzung von verschlüsselten Karten ausgelegt ist, beabsichtigen wir in Kooperation mit unseren Backend-Partnern die nötige Firmware zu entwickeln, um eine sicherere Zuordnung des Nutzers zu gewährleisten.

Die dritte angesprochene Schwachstelle hat der CCC wie folgt beschrieben: *„Auch die Kommunikation zwischen den Ladesäulen und dem Abrechnungs-Backend ist schlecht geschützt: Die Kartennummer wird auch hier – oft sogar ohne jegliche Verschlüsselung – direkt an den Anbieter übermittelt. Mit geringem technischem Aufwand kann man diese Kommunikation abfangen und so die Kartennummern von Kunden ernten. Aus diesen kann man dann entweder Ladekarten fälschen oder – in der Praxis wohl einfacher – gegenüber dem Ladenetzbetreiber Ladevorgänge simulieren“.*
Das vom CCC kritisierte OCPP 1.5 auf Basis von SOAP via HTTP stellt in der Tat einen unverschlüsselten Kommunikationskanal dar. Weil die Kommunikation zwischen unseren Ladestationen und den Backends allerdings nicht über das freie Internet, sondern über einen eigenen Zugangspunkt für Datenübertragung (APN) in einem separaten Machine-to-Machine (M2M) Netzwerk geschieht, sind ein Abgriff und die Manipulation von Daten nicht einfach möglich.

ABL SURSUM Bayerische Elektrozubehör GmbH & Co. KG
Geschäftsführer: Dr. Stefan Schlutius, Sabine Spiller-Schlutius
Registergericht Nürnberg HRA 6778
Komplementär: ABL SURSUM Bayerische Elektrozubehör Verwaltungs-GmbH
Registergericht Nürnberg HRB 4335
Albert-Büttner-Str. 11
91207 Lauf/Pegnitz
info@abl.de
T +49 9123 188 0
F +49 9123 188 188
www.abl.de
USt-IdNr. DE 132 809 180
ILN 40 11721 00000 8
WEEE-Reg.Nr. DE54480074

ABL

Lauf, 04.01.2017

Stellungnahme zur Sicherheit unserer Ladesäulen (2/2)

Die Produkte der ABL bieten auch den Transport der Nachrichten via Websockets und einer Verschlüsselung mit SSL an. Dieser Transport muss jedoch auch vom Backend unterstützt werden. Dieses Vorgehen entspricht den Anforderungen von OCPP 1.6, welches in Zukunft von unseren Ladestationen ebenfalls unterstützt wird.

ABL SURSUM Bayerische Elektrozubehör GmbH & Co. KG
Geschäftsführer: Dr. Stefan Schlutius, Sabine Spiller-Schlutius
Registergericht Nürnberg HRA 6778
Komplementär: ABL SURSUM Bayerische Elektrozubehör Verwaltungs-GmbH
Registergericht Nürnberg HRB 4335
Albert-Büttner-Str. 11
91207 Lauf/Pegnitz
info@abl.de
T +49 9123 188 0
F +49 9123 188 188
www.abl.de
USt-IdNr. DE 132 809 180
ILN 40 11721 00000 8
WEEE-Reg.Nr. DE54480074