EV Charging Security: the OCPP Security Operations Guide

Lonneke Driessen, OCA



OCPP Security Operations Guide

Canberra

October 21st, 2026

OCA Working Groups

Technology Working Group



Compliancy Working Group



Regional & Regulatory Requirements Working Group



Cybersecurity Task Group



Networking Task Group



Commissioning Task Group



Why is EV Charging Infrastructure Security important?



Charging Infrastructure can be a target for:

- Ransomware (chargers are expensive!)
- Data breaches
- Payment manipulation
- Industrial espionage
- Denial of Service
- Electricity grid manipulation via load manipulation
- Transportation sabotage
- …….

And the impact is only increasing!

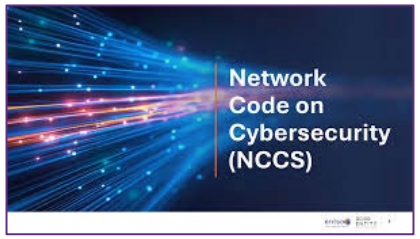
The good news: there is a lot of regulation!

MID
Measuring Instrument Directive
2014/32/UE







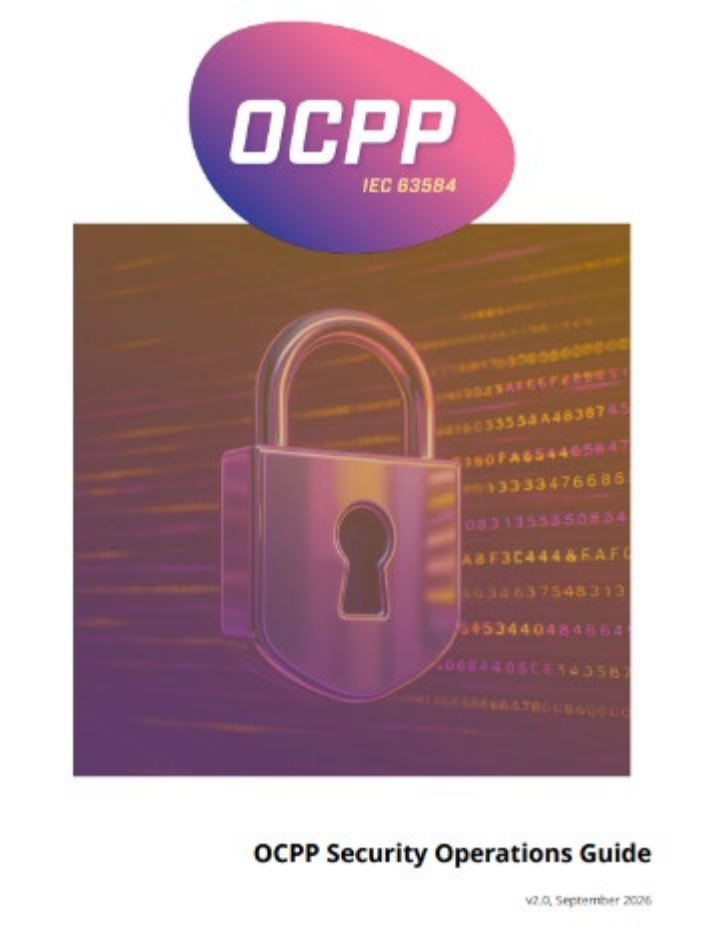






OCA
Open Charge Alliance

To help the industry, OCA has published a OCPP Security Operations Guide – for OCPP and beyond



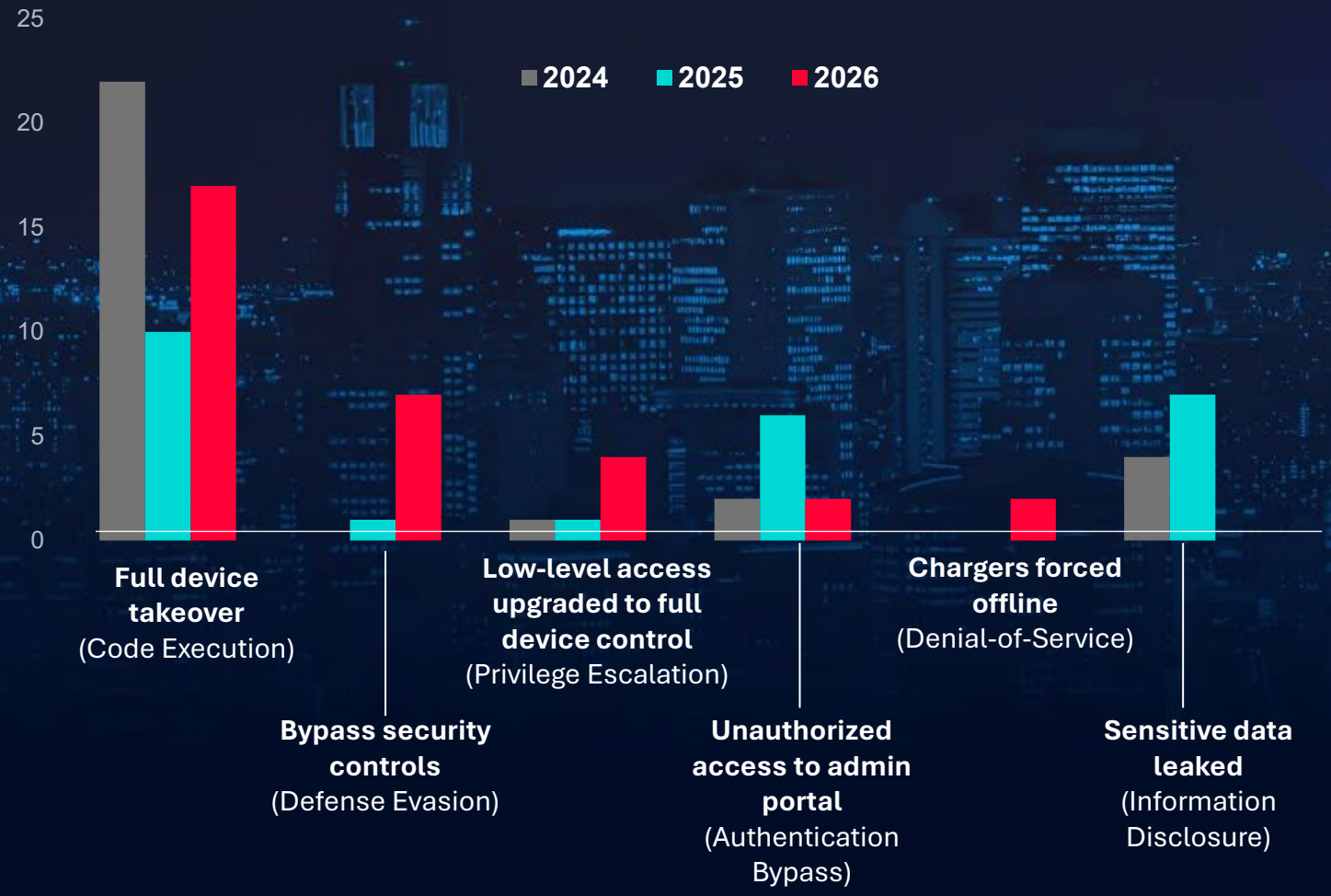
- **Regulations** vs. security measures (Europe, USA, Japan)
- **Guidance** for the industry
  - Explanation
  - 230 concrete requirements!
- **Real life data**: overview of security issues found in chargers

OCA
Open Charge Alliance

PWN2OWN AUTOMOTIVE



Impact











VicOne | ZERO DAY INITIATIVE

PWN2OWN AUTOMOTIVE

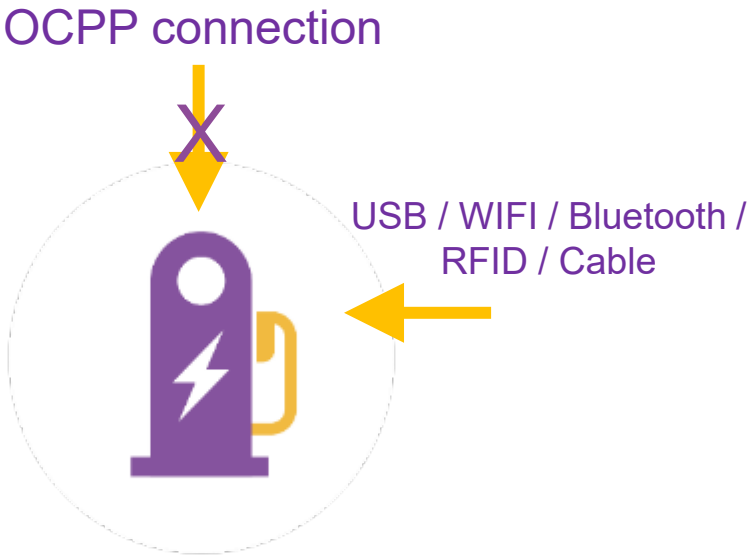
Total: 96 zero-day vulnerabilities identified for EV chargers from 2024 to 2026

OCA entered Pwn2Own Automotive 2026 with our testing tool OCTT, to get firsthand experience

- OCTT was not selected as a target!



- Charging Stations were targeted
- Via all interfaces, except OCPP!



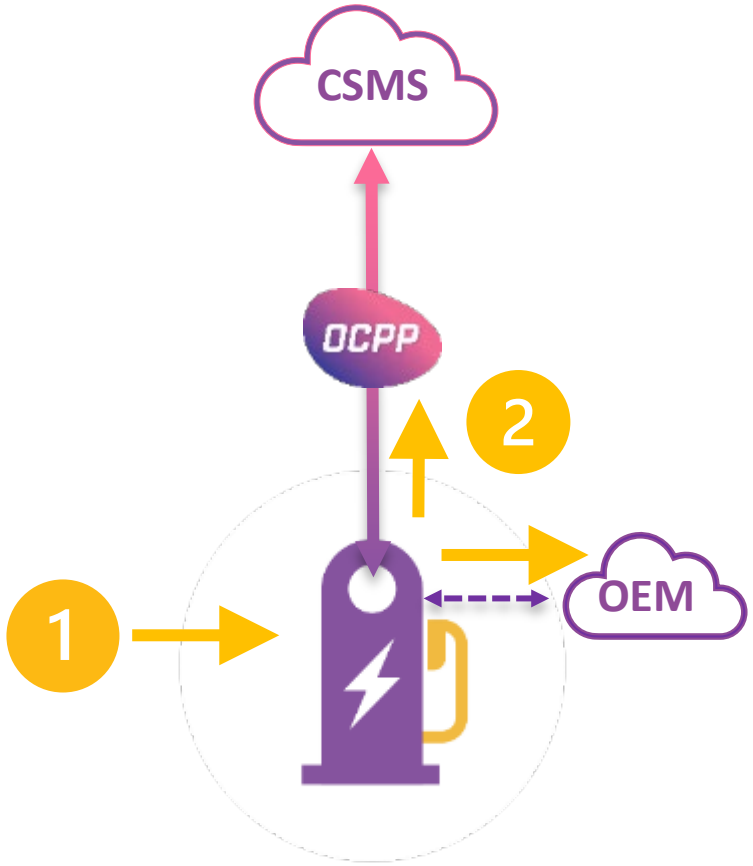
OCA is working with the best researchers to improve awareness and security in our industry



We plan to step up the game in 2027!

(currently under discussion)

- To include an ‘OCPP add on’ towards cloud systems
- Once researchers achieve code execution on the charging station…….
- ….they will try for code execution in the CSMS!



An official website of the United States government Here's how you know

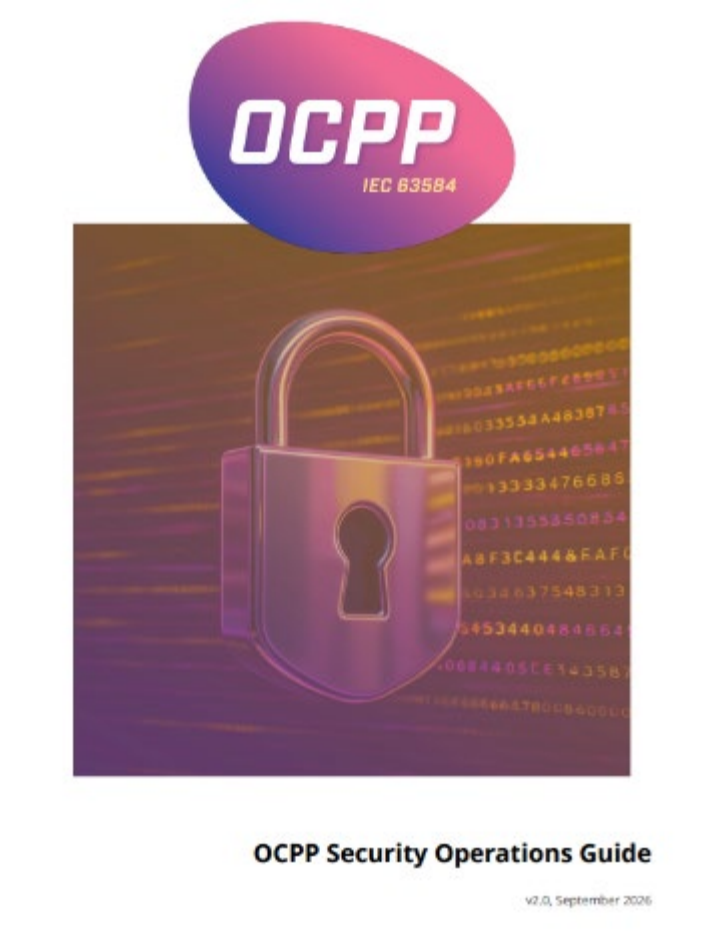
NVD Vulnerability Search

ocpp

Advanced Reset Show Statistics

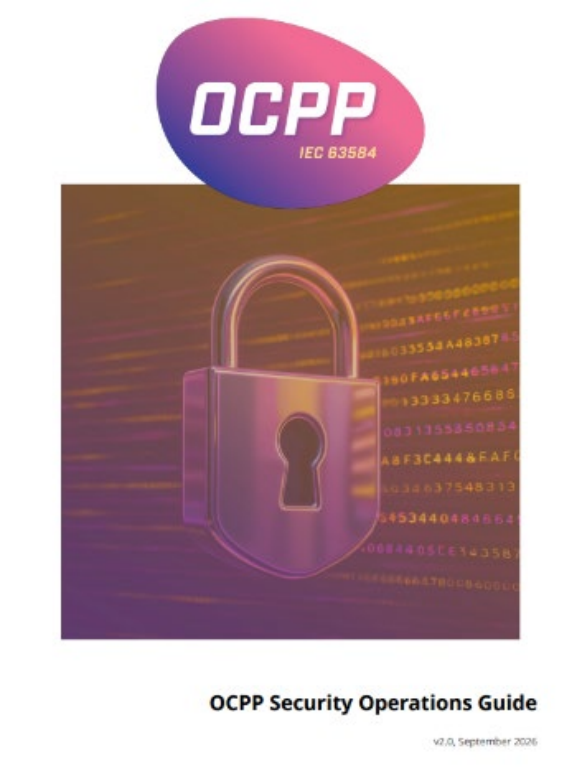
Identifier	CISA Kev Info	Published Date	CNA	Description
CVE-2026-26288	✖	2026-03-06	ICS-CERT	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then is...
CVE-2026-26051	✖	2026-03-06	ICS-CERT	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then is...
CVE-2026-				WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized

OCA continues to update the OCPP Security Operations Guide – a version 3!



- **Vulnerabilities** found via disclosures, Pwn2Own etc
- **Regional Security regulations**
  - Korea
  - No request for Australia yet!
- **Security Certification program**: inventory of which certifications would exhaustively cover all the requirements

Help us improve EV Charging Infrastructure security!



OCA is helping the industry by:

- creating awareness
- identifying concrete and actionable measures
- offering testing and certification
- handling vulnerability disclosures

How can you help OCA?

Help us improve EV Charging Infrastructure security!

How can you help?

1. Support OCPP
2. Support testing & certification for EV Charging Infrastructure
3. Support a coordinated approach to Vulnerability Research, Vulnerability Disclosures and corrective measures


Join the OCA
community!