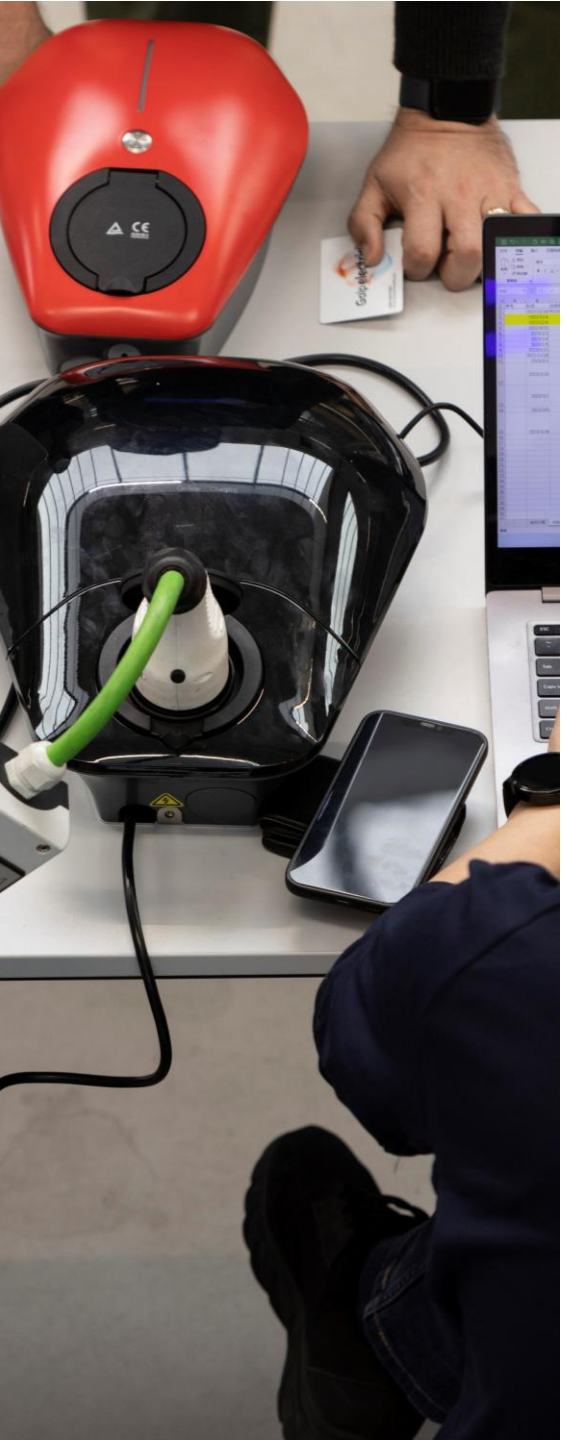
NLR Open Worldwide Application Security Project

Rens Willemsen
Open Charge Alliance

Top 10 weaknesses in EVSE

Rens Willemsen – Open Charge Alliance

Blueprint: Open Worldwide Application Security Project Top 10 Common Weakness Enumerations for Electric Vehicle Supply Equipment



Method and content

- Researchers used a similar approach as the OWASP top 10
- Top 10 made on basis of:
  - Frequency of the reported weakness
  - Seriousness of the potential impact
  - Wideness of the potential impact

Every weakness is described with:

- Exploitations
- Methods of prevention
- CWE's (Common weakness enumerations)

Communication Network Security

- Exploitations:
  - Interception of communication packets
  - Inject of excessive traffic
- Prevention:
  - Adopt with strong security mechanisms
  - Disable unnecessary network services
  - Validate with conformance testing

Authentication and Authorization

- Exploitations:
  - Using default credentials
  - Upload code to a Public GitHub
- Prevention:
  - Store credentials properly and change default credentials
  - Divide application in multiple access levels
  - No Caching for sensitive pages

Firmware and Software

- Exploitations:
  - Remote code execution
  - Authorization bypass
  - Heap-based buffer overflow
- Prevention:
  - Implement secure boot process
  - Continious Firmware updates
  - Secure communication and authentication protocols

Physical Tampering and Unauthorized Access

- Exploitations:
  - Gain privileged access
  - Connection sniffing
  - Denial of services
- Prevention:
  - Secure the EVSE ports
  - Secure open ports with authentication
  - Shield EV-EVSE charging cable

Backend Cloud Systems

- Exploitations:
  - Phishing and Malware deployment
  - Injection of malicious code
- Prevention:
  - Security awareness
  - High level of security system (including detection and access controls)

Payment Systems

- Exploitations:
  - RFID Cloning
  - Sensitive information storage
  - Connection sniffing (certificates)
- Prevention:
  - Include PKI
  - Transitioning to Plug-and-Charge
  - Scrub storage from all payment information

Web Applications and API

- Exploitations:
  - Access due weak password policy
  - SQL Injection
- Prevention:
  - Regular reviews for weaknesses
  - Use Secure-by-design principles

Integration With Power Grid

- Exploitations:
  - Oscillations in grid frequency
  - False data injection
- Prevention:
  - Proactive monitoring and incident response
  - Follow established cybersecurity standards and regulations
  - Implement smart charging techniques

Data Security and Privacy

- Exploitations:
  - Manipulate data enabling free charging
  - Data breach due insecure storage
  - Poorly secure smartphone applications for charging management
- Prevention:
  - Use end-to-end encryption
  - Use Secure communication protocols
  - Only store necessary data

Supply Chain

- Exploitations:
  - Back-doored firmware from third party vendor
  - Tampered chip with malicious embedded codes
  - Compromise of SDK or library

- Prevention:
  - Having and understanding of the product's software bill-of-materials and hardware-bill of materials
  - Implementing secure-by-design-principles all over the supply chain
  - Comply with industry standards

Conclusion

Charging infrastructure is getting smarter and more interconnected, this brings complexity which causes potential cyber security weaknesses. For a safe expansion of EV all sectors involved should address the interconnected cybersecurity vulnerabilities in EVSE with a comprehensive, multilayered security approach.