VicOne

Illuminating the Threat Landscape of Electric Vehicle Supply Equipment (EVSE) Infrastructure: Threat from the Dark Web and Zero-Day Threats

The Road Ahead: Looming Threats Over EVSE

As electric vehicle (EV) adoption accelerates, EV charging infrastructure has become deeply integrated with national and local power grids. EV chargers, e-Mobility Service Providers, their cloud ecosystems, along with connected vehicles, are attracting DIY enthusiasts and curious cybercriminals. This report outlines the current threat landscape, identifies key attack surfaces, and highlights the security implications of vulnerabilities in EV charging systems. A strategic partnership between VicOne and regulation entities would bolster national preparedness and secure EV deployment.

VicOne has outlined a forecast for EVSE cybersecurity threats within 5 years, according to the trends observed. Risks include data breaches over unencrypted channels, credential spoofing, low-tech hacking tools, ransomware on EV chargers, and physical risks caused by low-tech criminals and civilians trying to hack an EVSE. Underground criminals and nation-state actors would finally set foot in EV charging infrastructure.

Mapping Today's Threat Landscape: Understand What Could Go Wrong

The threat landscape in Electric Vehicle Supply Equipment (EVSE) and associated services is evolving along with the deployment of 192,000 charging ports in the U.S. [1] There were no significant observations of state-sponsored actors or Advanced Persistent Threats (APTs) targeting EVSE, while the presence of **ransomware**, **free-charging hacks**, and other fraudulent activities necessitates a proactive approach to securing the infrastructure.

- **Cybercriminal Activities:** Discussions have emerged in automotive forums whether credit card skimmers are capable ofstealing credit card details at EV charging stations. However, due to membership-based model adopted by many e-mobility service providers (eMSPs), no such incidents have been reported to date. Criminal activities specifically linked to EVSE remains limited, except for a few cases in China where individuals exploit loopholes to charge their EVs for free. There have also been instances where some individuals used stolen credit cards to buy and resell home EV chargers due to their high resale value.

- **Ransomware and Data Breaches:** While there have been no reports of direct attacks on EVSE yet, a Tesla charging database with PII was breached in November 2024 and a successful case in Pwn2Own Automotive 2024 competition where researchers successfully demonstrated an exploit against an EVSE provider that had embedded an AWS access key in the charger, creating the potential for unauthorized access to PII and other sensitive data.

- **Phishing and Scams:** Phishing has not been prominently observed in relation to EVSE, but a local government authority in the United Kingdom warned the public on the use fraudulent QR codes. These malicious codes redirect users to fake payment portals, enabling payments to fraudulent accounts instead of the government.

- **Research-Identified Vulnerabilities:** Academic research has highlighted protocol vulnerabilities such as OCPP and ISO 15118, with particular emphasis on attack vectors transmitted through charging cables. [2]

- **Denial of Service (DoS) and Communication Disruptions:** DoS attacks have been discussed in academic literature, focusing on protocol-level exploits and side-channel radio disruptions. While such attacks have not yet been observed in the wild, their technology remains simple. However, the Telstra outage in June 2024 [3] illustrates the real-world impact of communication disruption, where numerous ChargeFox stations ceased operation due to their inability to maintain connectivity with backend charging servers.

- **Insider Threats:** A former operations manager of a Chinese EV charging station was caught using “engineering mode” with administrator’s password to freely charge his and friends’ EVs without authorization. A similar incident happened in China where a flaw in the business logic of an EV charging app inadvertently allowed users to access charging services free of charge.

- **Physical Threats and Vandalism:** Seven Tesla charging poles were reportedly destroyed in a politically motivated arson incident. [4] Despite this case, there have been no reports of vandalism or major physical threats against EVSE.

- **Grid Manipulation:** Several academic studies have explored the potential for electric vehicle charging infrastructure to be leveraged in grid destabilization scenarios, but no incidents have been reported or observed yet. However, as a precautionary measure, selling Wallbox Copper SB home charger was prohibited in the United Kingdom. [5]

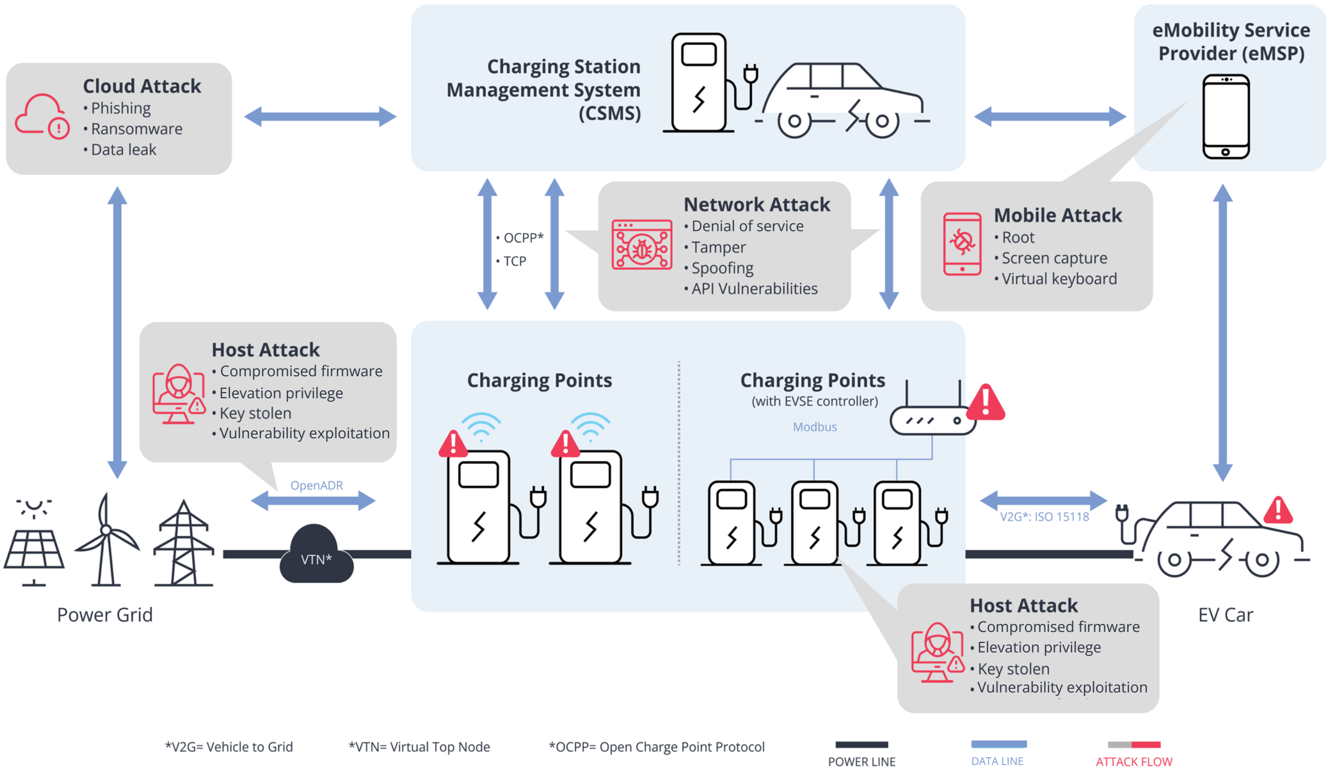
The current threat landscape for EVSE and related services is characterized by emerging and potential threats. While these are neither immediate nor widespread, proactive and focused attention is essential to mitigate vulnerabilities and strengthen the cybersecurity posture of the EV ecosystem.

Attack Vectors: Understanding Key Entry Points

The attack vectors targeting EVSE and infrastructure have remained largely consistent since the publication of pivotal research papers, such as those from Sandia National Laboratories and Southwest Research Institute [6] [7] Threats were extensively explored and validated in Pwn2Own Automotive 2024 and 2025.

The attack vectors expanded from the signal lines (physical and radio tampering), programmable logic control (PLC) vulnerabilities to unencrypted connection, unsanitized user input, exposed services on LAN or even WAN, and firmware vulnerabilities. Notably, most charging stations assessed during Pwn2Own Automotive lacked modern security mechanisms such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), stack canaries, and rigorous input validation. The level of EVSE protection remains comparable to that of a personal computer in the 1990s.

Attack Surface in EVSE



Charging Hardware

A few EVSE providers have JTAG enabled on the PCB, with which researchers can dump firmware and even interface it to GDB and debug the internal states.

Charging Firmware and Remote Update

One case in Pwn2Own Automotive showed that OTA update of the firmware can be tampered with. It is almost always possible to extract the firmware if the EVSE can be obtained / purchased.

Charging Interfaces

A number of academic research papers focused on EV couplers, user terminals, backhaul connections, and maintenance interfaces [7] on EVSE. Moreover, insider threat scenarios have been observed, where individuals input fixed administrator PIN codes [8] or use an app with invalid logic [9]. One researcher used a radio signal to jam the signal on the charging cable.

Protocol vulnerabilities

A research paper spoofed CCS message at Control Pilot (CP), thus changing the charging current and causing denial of service. [6]

Backend systems

E-mobility service providers could be breached or ransomed. IntelBroker claimed to have breached Tesla Charging Database. Sample data was given on Breach Forums. A shared SSH key was found in Pwn2Own Automotive 2024 which led back to the vendor's cloud, exposing S3 buckets which contained customer PII.

Exposed services

Internal services such as SSH, Telnet (without authentication), vulnerable HTTP servers, management interface with hardcoded credentials, etc., have been reported in academic papers and Pwn2Own Automotive 2024 / 2025. Exposed services in WAN and LAN are one of the most prominent attack vectors.

Operating system

While EVSE uses all sorts of operating systems, it is noteworthy that Gecko OS used in JuiceBox 40 suffered from a Telnet server without authentication and a few command-line injections. In Pwn2Own Automotive 2024 and 2025, vulnerabilities such as command-line injection over WiFi SSID, command injection over customized protocols, configuration injection over PPPD and DHCP, JSON type confusion, insecure firewall configuration, buffer overflow in system log printing, and heap- and stack-based buffer overflow were used to pwn the devices.

Unsanitized input and API entry point

In Pwn2Own Automotive 2024, a device was reported to allow changing the password without validating the old password. Another bug disclosed by Ryan of the Kilowatts in 2023 showed that an attacker can gain access via TeamViewer to Electrify America's EV charging stations. [10]

Unsecured communications

Data in all interfaces should be properly secured and encrypted. However, we see TCP packets in charging cables not always encrypted. Researchers could even connect to EVSE's internal services by hooking into the charge cable. [2] In Pwn2Own Automotive 2024, it is found in devices that Bluetooth Low Energy (BLE) has no authentication, unencrypted content over Bluetooth GATT, TLS hostname not verified thus causing OCPP messages to be intercepted, SSL certificate not validated as to allow forging WebSockets.

Supply chain / SBOM attacks

We have not spotted discussions on hardware supply chain attacks. With regards to software BOM, VicOne's xZETA scans firmware and finds outdated and vulnerable libraries.

Grid / V2G / V2X

There have been very limited discussions regarding attacks on the grid, the V2G interface, or the V2X interface. There are academic research papers [11], but not deep enough discussions in the Deep and Dark Webs.

Here is a list of devices being tested in Pwn2Own Automotive 2024 and Pwn2Own Automotive 2025, along with the attack vectors that were successfully exploited.

Pwn2Own Automotive 2024

	AUTEL MAXICHARGER AC WALLBOX COMMERCIAL	CHARGEPOINT HOME FLEX	EMPORIA EV CHARGER LEVEL 2	JUICEBOX 40 SMART EV	PHOENIX CONTACT CHARX SEC-3100	UBIQUITI CONNECT EV STATION
CWE-20		⊗ (WiFi SSID)			⊗ (DHCP, PPPD)	⊗ (API)
CWE-78		⊗		⊗ (HTTP)		
CWE-120					⊗	
CWE-121	⊗		⊗	⊗		
CWE-125					⊗	
CWE-134				⊗		
CWE-269					⊗	
CWE-295		⊗				⊗
CWE-284		⊗				
CWE-416					⊗	
CWE-620						⊗
CWE-668				⊗ (DHCP, PPPD)	⊗ (SSH)	
CWE-798	⊗				⊗	
CWE-843					⊗	
CWE-1191		⊗				

Pwn2Own Automotive 2025

	AUTEL MAXICHARGER AC WALLBOX COMMERCIAL	CHARGEPOINT HOME FLEX (MODEL CPH50)	PHOENIX CONTACT CHARX SEC-3150	TESLA WALL CONNECTOR	UBIQUITI CONNECT EV STATION	WOLFBOX LEVEL 2 EV CHARGER
CWE-78		X	X			
CWE-120	X (HTTP)					
CWE-121	X	X				
CWE-122	X					X
CWE-284	X					
CWE-295					X	
CWE-306				X		
CWE-321					X	
CWE-345	X					
CWE-346			X			
CWE-457						X
CWE-540			X			
CWE-749						X
CWE-798					X	X
CWE-839				X		
CWE-1328	X		X	X		

Please refer to Appendix B for a list of CWE.

Remarks on Regulation and International Standards

The vulnerabilities being found in Pwn2Own Automotive 2024 and 2025 are mostly on home chargers, except Phoenix Contact CHARX SEC-3xxx, which could be used in EV charging stations. However, the cybersecurity issues found in Pwn2Own Automotive if applied on EV charging infrastructure, should be addressed and mitigated by complying with regulations and the latest international standards, such as NIST IR 8473, IEC-62443, ISO-15118-20 and the latest OCPP 2.1.

The successful exploits at Pwn2Own Automotive illuminate why adherence to a single standard is insufficient and how these frameworks, while seemingly overlapping, are each essential in a defense-in-depth strategy. The attack's success stemmed from exploiting vulnerable EV to EVSE communication interface and targeting security flaws in firmware and the operating system, as well as in the device's proprietary management plane – specifically, the insecure firmware, firmware update process and unauthenticated APIs. This underscores the distinct and complementary roles of key standards.

ISO 15118-20 defines the high-level communication (HLC) between the EV and the EVSE, mandating the security of the business transaction through TLS encryption and Public Key Infrastructure (PKI). It protects the payment and data exchange process, but its scope does not extend to the device's underlying operating system or administrative functions. In contrast, **IEC 62443** addresses the EVSE's role as a critical infrastructure endpoint, focusing on Operational Technology (OT) security of the industrial control field. It provides requirements for firmware hardening, zone segmentation, and vulnerability management – precisely the areas exploited at Pwn2Own Automotive.

Furthermore, **ISO/SAE 21434 and UN R155** impose a legal obligation on OEMs and their supply chains, mandating a comprehensive Cybersecurity Management System (CSMS) and a secure development lifecycle (SDLC) for vehicles and their components. This creates accountability that might extend to the EVSE supply chain.

NIST IR 8473 ties these elements together. It acts as an actionable cybersecurity framework profile tailored for the fast-charging/EVSE ecosystem, translating broad frameworks like NIST SP 800-53r5, PCI-DSS, and IEC 62443 into a verifiable checklist mapped across four key domains: EV, EVSE, Cloud, and the Utility Grid. By providing this practical implementation guide, it lowers the barrier for manufacturers to adopt a holistic security posture. The Pwn2Own Automotive events are a definitive proof that securing the EVSE ecosystem requires this integrated approach, where secure transactions (ISO 15118-20), robust industrial controls (IEC 62443), and accountable development lifecycles (ISO/SAE 21434) are all orchestrated under a unified, risk-based framework.

For more information on the regulations and international standards, please refer to VicOne's whitepaper "Pwn2Own Automotive 2024 Findings on EVSE Controllers: A regulation perspective".

Intelligence from the Clear Web (Foresight ATS)

There have been limited numbers of news and incidents on the clear web since 2024. VicOne threat intelligence team plans to extend sourcing of EVSE in Q3'25.

Here is a list of topics and research being discussed on the clear web.

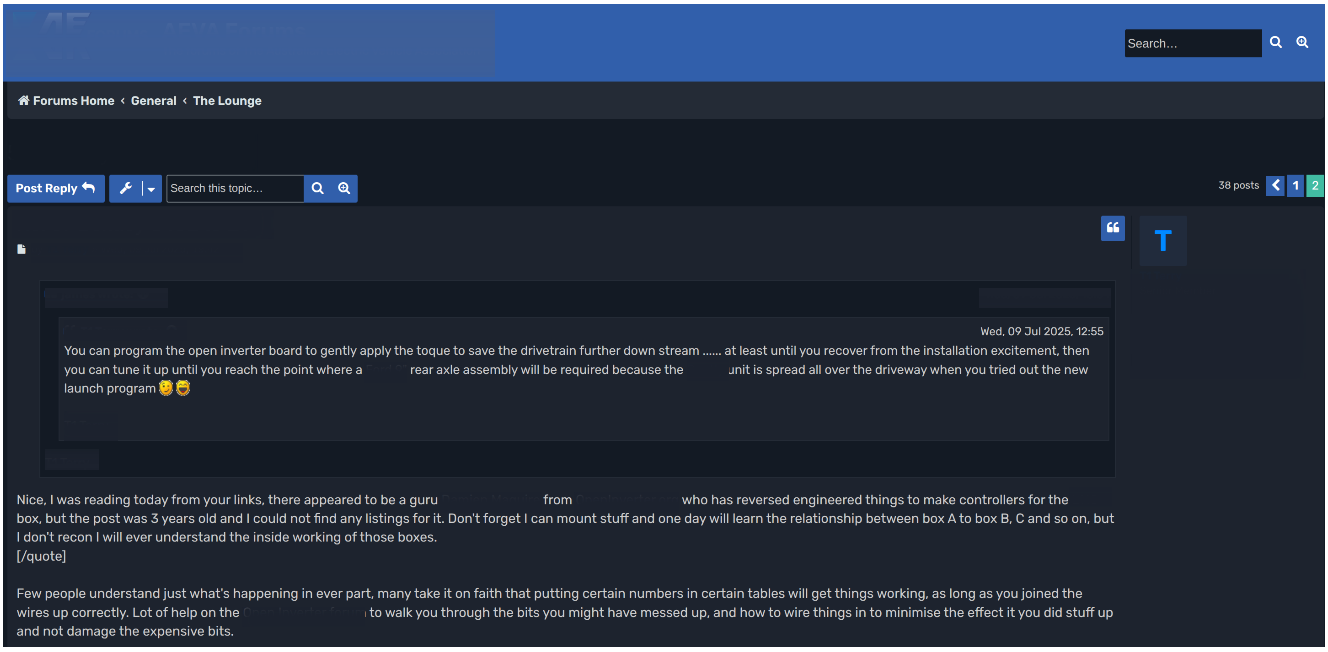
- Building an electric vehicle simulator to research EVSEs
- Cyber defense in OCPP for EV charging risks
- Innovative investigation of the resilience of EV charging infrastructure under cyber-physical threats based on a real-time co-simulation testbed [12]
- 44CON – Charging Ahead: Exploiting an EV Charger Controller at Pwn2Own Automotive 2024
- Hacking EV Charging Point, for fun ... and fixing the firmware
- Hacking EV charging stations via the charging cable
- Security Advisory: Critical Vulnerabilities in EV Charging Stations: Analysis of eCharge Controllers
- The team from Synacktiv used a logic bug as a part of their chain to exploit the Tesla Wall Connector via the Charging Connector.
- Nissan Leaf recalled for possible battery fire while fast charging
- Demonstration of denial of charging attack on electric vehicle charging infrastructure and its consequences
- Leading EV charging network hampered by Telstra outage

Deep and Dark Web (xAurient)

VicOne threat intelligence team collects data from deep web and dark web, as well as purchases external data sources that monitor deep- and darkweb.

There are limited discussions on EVSE other than normal usage and home chargers. Several topics include user reports and solutions on charging issues, electrical system compatibility issues and charging challenges, complaints about Integrated Charging Control Unit (ICCU), and safety risks highlighted in improper installation of electric vehicle charging stations.

Among the sources, we noted that in July, 2025, a car owner shared how they changed their [redacted] The modification might not comply with federal and/or state regulations. VicOne xAurient provides source links to the original post when it's feasible.



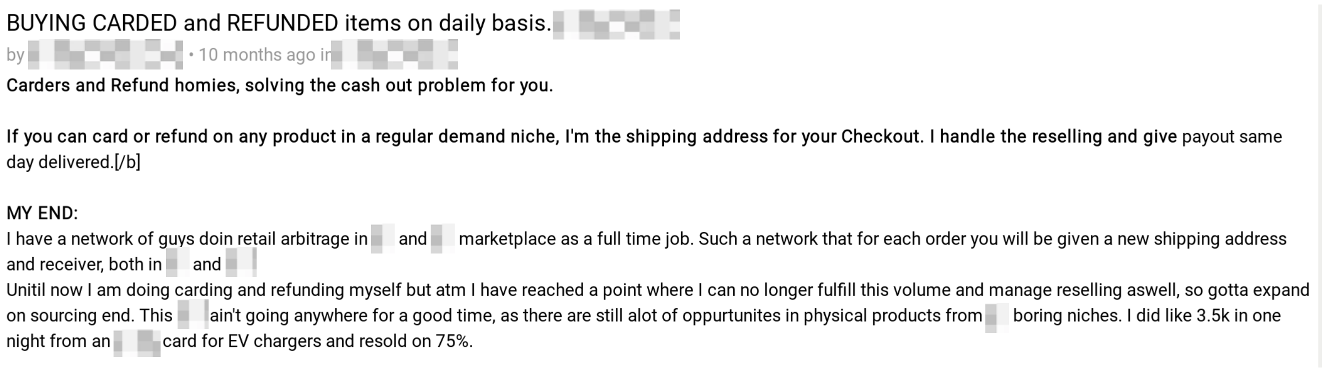
Wed, 09 Jul 2025, 12:55

You can program the open inverter board to gently apply the toque to save the drivetrain further down stream ...... at least until you recover from the installation excitement, then you can tune it up until you reach the point where a [redacted] rear axle assembly will be required because the [redacted] unit is spread all over the driveway when you tried out the new launch program 😉😎

Nice, I was reading today from your links, there appeared to be a guru [redacted] from [redacted] who has reversed engineered things to make controllers for the box, but the post was 3 years old and I could not find any listings for it. Don't forget I can mount stuff and one day will learn the relationship between box A to box B, C and so on, but I don't recon I will ever understand the inside working of those boxes.
[/quote]

Few people understand just what's happening in ever part, many take it on faith that putting certain numbers in certain tables will get things working, as long as you joined the wires up correctly. Lot of help on the [redacted] to walk you through the bits you might have messed up, and how to wire things in to minimise the effect it you did stuff up and not damage the expensive bits.

There are few discussions on EVSE in the dark web, as it remains relatively new to cybercriminals. We have spotted one carder (people who steal credit card numbers and make a profit) using stolen credit cards to buy and resell home EV chargers, because they are expensive and easy to sell.



BUYING CARDED and REFUNDED items on daily basis.[redacted]

by [redacted] • 10 months ago in [redacted]

Carders and Refund homies, solving the cash out problem for you.

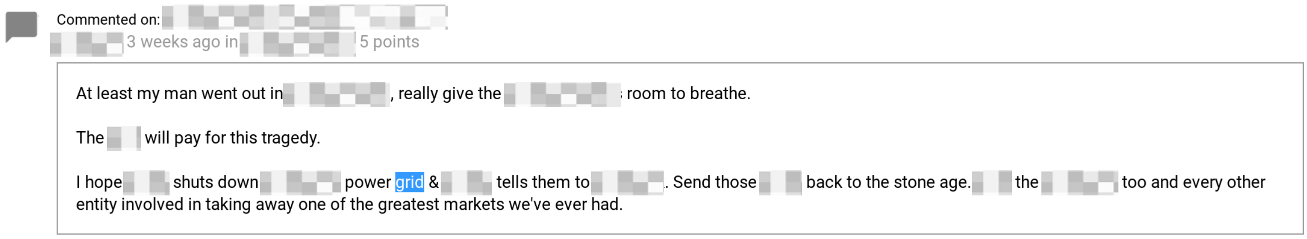
If you can card or refund on any product in a regular demand niche, I'm the shipping address for your Checkout. I handle the reselling and give payout same day delivered.[/b]

MY END:

I have a network of guys doin retail arbitrage in [redacted] and [redacted] marketplace as a full time job. Such a network that for each order you will be given a new shipping address and receiver, both in [redacted] and [redacted]

Unitil now I am doing carding and refunding myself but atm I have reached a point where I can no longer fulfill this volume and manage reselling aswell, so gotta expand on sourcing end. This [redacted] ain't going anywhere for a good time, as there are still alot of oppurtunites in physical products from [redacted] boring niches. I did like 3.5k in one night from an [redacted] card for EV chargers and resold on 75%.

One person threatened to shut down [redacted] power grid. But it was a lame threatening without detail.



Commented on: [redacted]

[redacted] 3 weeks ago in [redacted] 5 points

At least my man went out in [redacted], really give the [redacted] room to breathe.

The [redacted] will pay for this tragedy.

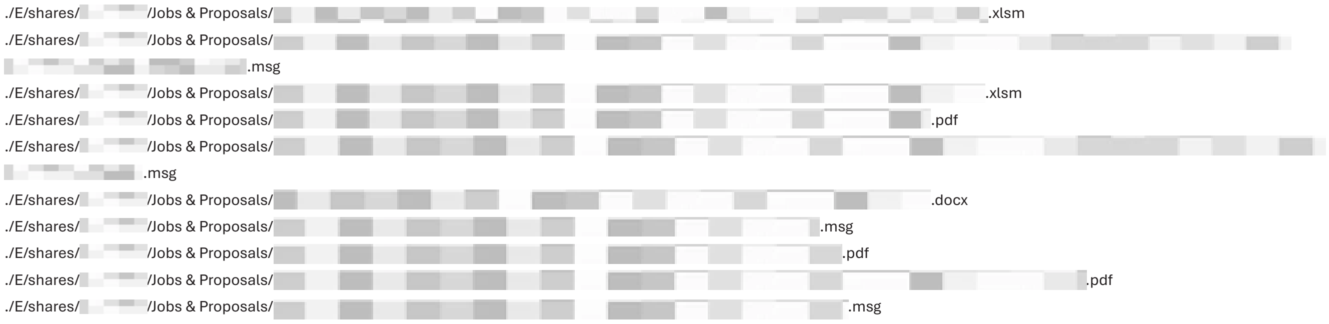
I hope [redacted] shuts down [redacted] power grid & [redacted] tells them to [redacted]. Send those [redacted] back to the stone age. [redacted] the [redacted] too and every other entity involved in taking away one of the greatest markets we've ever had.

Someone asked how to shut down the U.S. power grid two years ago, but people on the dark web did not welcome the question. [15]

No attacks on the EV charger were spotted.

VicOne also monitors ransomware groups in the darkweb. On July 17, 2025, Nitrogen ransomware group breached C3 Group and made the stolen data public.

We have noticed a few documents on a tender for [redacted] We did not retrieve the documents for legal reasons.



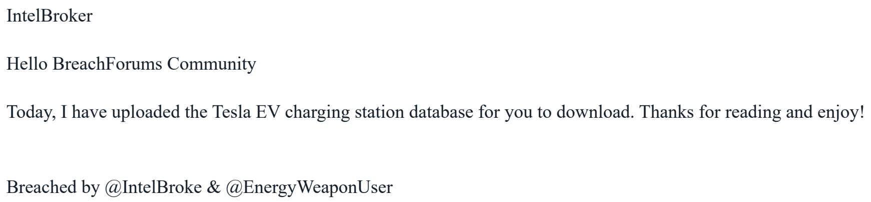
```
./E/shares/[redacted]/Jobs & Proposals/[redacted].xlsm
./E/shares/[redacted]/Jobs & Proposals/[redacted]
[redacted].msg
./E/shares/[redacted]/Jobs & Proposals/[redacted].xlsm
./E/shares/[redacted]/Jobs & Proposals/[redacted].pdf
./E/shares/[redacted]/Jobs & Proposals/[redacted]
[redacted].msg
./E/shares/[redacted]/Jobs & Proposals/[redacted].docx
./E/shares/[redacted]/Jobs & Proposals/[redacted].msg
./E/shares/[redacted]/Jobs & Proposals/[redacted].pdf
./E/shares/[redacted]/Jobs & Proposals/[redacted].pdf
./E/shares/[redacted]/Jobs & Proposals/[redacted].msg
```

External Sources

VicOne threat intelligence team collects external sources whenever there is a request for information. There are reports claiming that consumers were targeted by fraudulent QR codes at EV charging stations and parking meters. In April 2025, a local UK government warned that threat actors targeted contactless payment hotspots and placed their own QR codes on the signage. [16]

On Dec 4, 2024, Z-PENTEST ALLIANCE group (a pro-Russia hacker group) claimed responsibility for attacks at a South Korea-based electric car charging station. (Telegram channel, source already vanished.)

On Nov 19, 2024, the actor IntelBroker shared a download link for a dataset that allegedly impacted the India-based software company Numocity Technologies Private Ltd. on the Breach Forums (shutdown in June 2025). They claimed the compromised dataset contained information pertaining to Tesla electric vehicle (EV) charging stations in the Middle East, and specifically the UAE. The breach allegedly took place in November 2024 and exposed 116,000 rows of customer information such as full names, locations, payment information, vehicle identification numbers (VINs), and vehicle information.



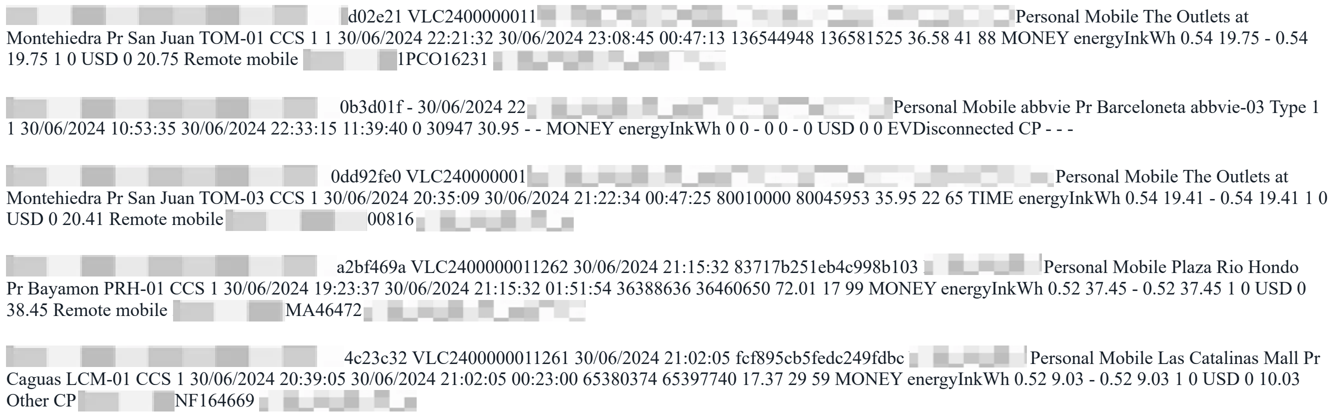
IntelBroker

Hello BreachForums Community

Today, I have uploaded the Tesla EV charging station database for you to download. Thanks for reading and enjoy!

Breached by @IntelBroke & @EnergyWeaponUser

Sample Data:



```
[redacted] d02e21 VLC2400000011[redacted] Personal Mobile The Outlets at
Montehiedra Pr San Juan TOM-01 CCS 1 1 30/06/2024 22:21:32 30/06/2024 23:08:45 00:47:13 136544948 136581525 36.58 41 88 MONEY energyInkWh 0.54 19.75 - 0.54
19.75 1 0 USD 0 20.75 Remote mobile [redacted] 1PCO16231 [redacted]

[redacted] 0b3d01f - 30/06/2024 22[redacted] Personal Mobile abbvie Pr Barceloneta abbvie-03 Type 1
1 30/06/2024 10:53:35 30/06/2024 22:33:15 11:39:40 0 30947 30.95 - - MONEY energyInkWh 0 0 - 0 0 - 0 USD 0 0 EVDisconnected CP - - -

[redacted] 0dd92fe0 VLC240000001[redacted] Personal Mobile The Outlets at
Montehiedra Pr San Juan TOM-03 CCS 1 30/06/2024 20:35:09 30/06/2024 21:22:34 00:47:25 80010000 80045953 35.95 22 65 TIME energyInkWh 0.54 19.41 - 0.54 19.41 1 0
USD 0 20.41 Remote mobile [redacted] 00816 [redacted]

[redacted] a2bf469a VLC2400000011262 30/06/2024 21:15:32 83717b251eb4c998b103 [redacted] Personal Mobile Plaza Rio Hondo
Pr Bayamon PRH-01 CCS 1 30/06/2024 19:23:37 30/06/2024 21:15:32 01:51:54 36388636 36460650 72.01 17 99 MONEY energyInkWh 0.52 37.45 - 0.52 37.45 1 0 USD 0
38.45 Remote mobile [redacted] MA46472 [redacted]

[redacted] 4c23c32 VLC2400000011261 30/06/2024 21:02:05 fcf895cb5fedc249fdbc [redacted] Personal Mobile Las Catalinas Mall Pr
Caguas LCM-01 CCS 1 30/06/2024 20:39:05 30/06/2024 21:02:05 00:23:00 65380374 65397740 17.37 29 59 MONEY energyInkWh 0.52 9.03 - 0.52 9.03 1 0 USD 0 10.03
Other CP [redacted] NF164669 [redacted]
```

Threat Evolution and Predictions

The deployment of EVSE has surged with standardized charging protocols such as CCS1, CCS2, GB/T 20234, Type 1, Type 2, ChaDeMo, and NACS being widely adopted across many countries. However, the rapidly evolving technology and the wide development of EV charging services make it hard to accurately predict the threat landscape of EVSE in the future Based on the intelligence that VicOne threat intel team has collected, we anticipate several cybersecurity risks that may occur in the next 3-5 years.

Unencrypted customer data, including Vehicle Identification Numbers (VIN), transaction IDs, and charging locations, leads to data breaches, which could enable criminals to **spoof legitimate users'** VINs and credentials using the leaked information. Furthermore, the emergence of **"Hack-in-a-Box"** tools, exploiting **data frame injection** on charging cables and plugs, may become accessible to low-tech criminals, facilitating unauthorized access to EV charging systems.

Ransomware attacks may manifest as **ransom notes** displayed on EV chargers, akin to incidents observed with banking ATMs. Additionally, roadside charging stations may become targets for carders seeking to install **credit card skimmers**. **Remote** EV charging stations could serve as entry points for further cyberattacks on infrastructure, leading to **deeper breaches**, lateral movements, and the deployment of **rootkits** on eMobility Service Providers' (eMSPs) backend and cloud services.

Physical vulnerabilities may also be exploited by criminals **unscrewing** EV charging station lids to upload malware, profiting from immediate free charging or by selling **"criminal free-charging VIP cards."** The fraudulent "free-charging" or "extra-discount" **apps** could scam car owners, while reverse engineering of charging apps might reveal more creative vulnerabilities that facilitate free charging and breaches of PII.

The EV charging industry will grow to the point where it becomes too attractive for cybercriminals all over the world to ignore. **Nation-state actors** might already be roaming inside EV charging infrastructures, but their actions will become more explicit and observable for both financial and political gains. These actors may also study home EV chargers to induce **local blackouts** or **cascading failures**, as these devices are often less maintained and vulnerable to hacking.

Local power grid blackouts, instigated by nation-state actors or extreme activists, could impact critical services, including hospitals and 911, potentially **costing lives**. Moreover, physical theft of electricity from EVSE may lead to electric shock and fatalities. Unregulated third-party charging components and chips, deteriorated Integrated Charging Control Units (ICCU) and Battery Management Systems (BMS), could also result in **vehicle accidents and fires.**

Last but not least, time-synchronization-based and other innovative attacks might take place on individual EV charging stations.

Some of the predicted cybersecurity risks can be effectively mitigated if EVSE manufacturers follow cybersecurity best practices. Proper implementation of encrypted protocols, regular security audits, and incident response plans are essential in safeguarding the evolving EV charging infrastructure.

Conclusion and Mitigations

This threat intelligence report has reviewed the studies on EVSE in 2024 and 2025, VicOne's monitoring of clear, deep and dark webs, in addition to EV charging devices successfully breached in Pwn2Own Automotive 2024 and 2025. We want to call on the actions on the risks to the power grid, public safety, and car owners.

Grid Disruption

Compromising a certain number of fast-charging stations at the same time could destabilize the local grid. Coordinated attacks could lead to voltage fluctuations, load imbalances, frequency drifting, and consequently power outages. This might lead to local or widespread blackouts. Researchers are still estimating and finding ways to stabilize the grids and to prevent cascading failure. [17]

Public Safety Impacts

Malicious control over chargers could cause charging interruption and over-current. Even though it is a safety requirement for CCU and BMS in each EV to properly disconnect the power when the electricity goes beyond the specification, it is crucial to add anti-tampering elements to EV chargers or avoid using vulnerable protocols (such as PWM) to decide charging parameters.

Privacy and PII protection

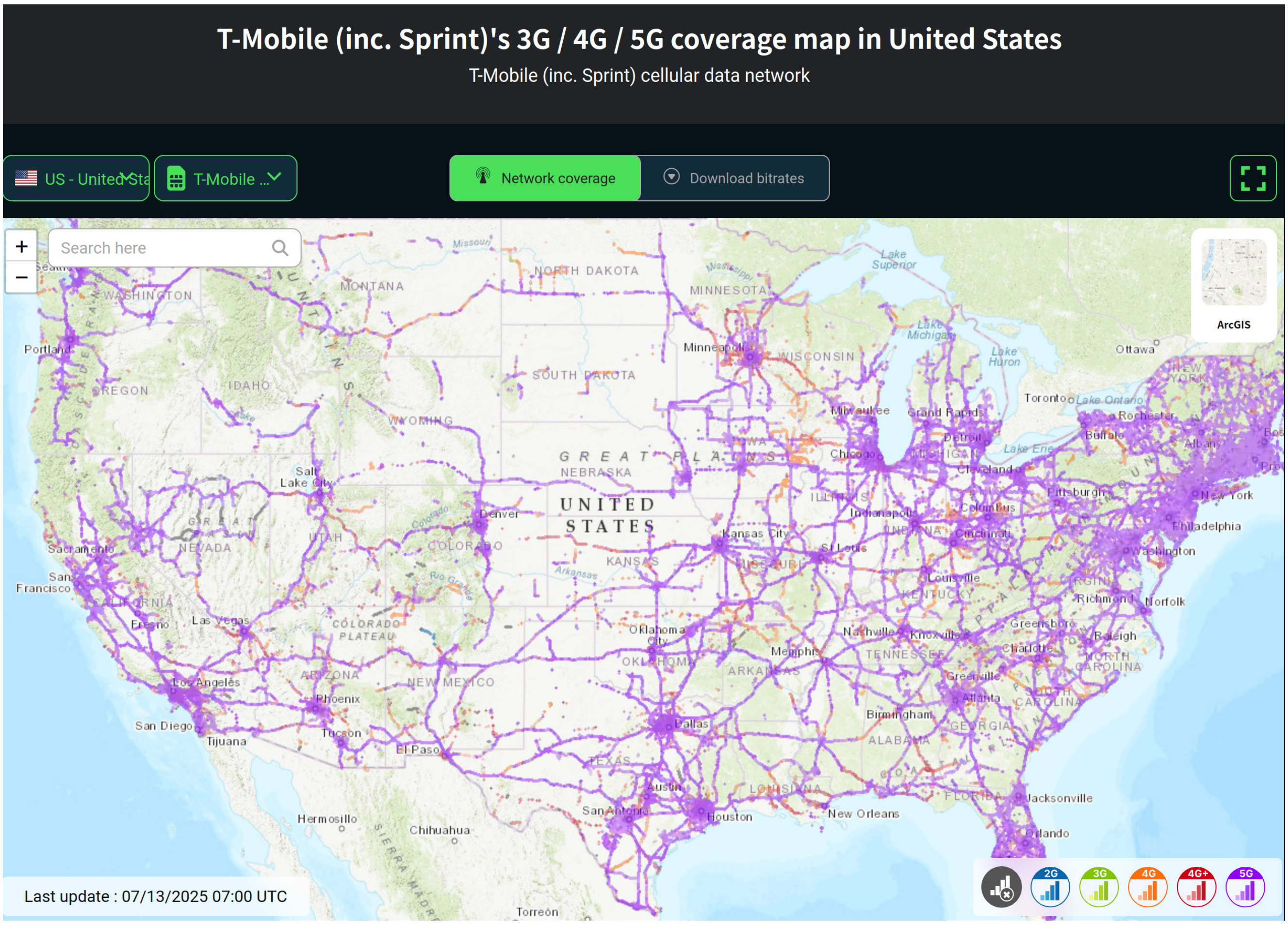
Insecure EV charging infrastructure enables attackers to track driver's charging locations, intercept payment data, steal credit card numbers, or interrupt vehicle charging sessions, posing both privacy violations and personal safety risks.

Following cybersecurity best practices, such as using IDS/IPS, network segmentation, proper configuration of firewalls, remote backup of auditing logs, and frequent applying of security patches, are crucial to securing EV charging infrastructure. VicOne has provided security platforms that facilitate firmware vulnerability scanning, cyberthreat intelligence monitoring and collection, IDS/IPS for EV and EV charging infrastructure.

The Value of Working with VicOne

VicOne Research Points

VicOne Threat Research team does security research on automotive and robotic appliances. We spot the possibility of communication spoofing via 2G/3G connected charging stations in remote areas. Even though most carriers have upgraded their cellular base stations to LTE and 5G, there are still a few unsecure base stations in remote areas.



T-Mobile (inc. Sprint)'s 3G / 4G / 5G coverage map in United States

T-Mobile (inc. Sprint) cellular data network

SBOM and Vulnerabilities (xZETA)

VicOne xZETA scans SBOM in customer-provided firmware. We have noted emerging vulnerabilities, such as PerfectBlue, and alerts when a component in SBOM is vulnerable.

VicOne monitors recent and older vulnerabilities.

Phoenix Contact: Security Advisory for CHARX SEC-3xxx Charging Controllers

The vulnerabilities can lead to a total loss of confidentiality, integrity, and availability of the devices. Affected charging controllers are designed and developed for use in closed industrial networks. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

Mitigation: Upgrade to firmware version 1.7.3
Source: https://certvde.com/de/advisories/VDE-2025-019/

Tencent X-in-the-Middle Attack on Tesla Pile
Source: https://www.rtl-sdr.com/tesla-charging-ports-opened-with-hackrf-replay-attack/

ZDI / Pwn2Own Automotive

VicOne works with Trend Zero Day Initiative™ (ZDI) and has early access to Pwn2Own Automotive findings, such as the Tesla Wall vulnerability exploited by Synacktiv.

In January 2024, we had the first edition of Pwn2Own Automotive and in January 2025 the second. Researchers around the world found nearly 50 previously unknown vulnerabilities impacting EV chargers, operating systems and IVI from entities including Alpine, Autel, ChargePoint, Kenwood, Phoenix Contact, Sony, Tesla, Ubiquiti and WolfBox.

Threat Intelligence and CyberThreat Research Teams

VicOne Threat Intelligence team monitors deep web and dark web for breaches, vulnerabilities, and unauthorized access of major eMSP companies, as well as criminal activities against carding / credit card skimming frauds against EV charging facilities.

We also find sources from the clear, deep, and dark webs. VicOne customers can assign keywords of their interests to receive immediate alerts and daily reports.

Penetration-Testing Team

VicOne PT team is currently testing Emperio Level 2 EV charger with break-throughs. They can help identify vulnerabilities on par with and beyond the case of ICSA-25-196-03 (store FTP-server access credentials in cleartext).

Appendix A – CVEs Assigned to Pwn2Own Devices

2025

ZDI ID	CVE	CVSS v3.0	Published	Title
ZDI-25-628	CVE-2025-25271	3.1	2025-07-22	(Pwn2Own) Phoenix Contact CHARX SEC-3150 OCPP Authentication Bypass Vulnerability
ZDI-25-624	CVE-2024-25995	7.5	2025-07-21	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Command Injection Remote Code Execution Vulnerability
ZDI-25-623	CVE-2025-25270	6.3	2025-07-21	(Pwn2Own) Phoenix Contact CHARX SEC-3150 Origin Validation Error Firewall Bypass Vulnerability
ZDI-25-622	CVE-2025-25268	8.8	2025-07-21	(Pwn2Own) Phoenix Contact CHARX SEC-3150 Configuration Service Missing Authentication Vulnerability
ZDI-25-621	CVE-2025-25269	8.8	2025-07-21	(Pwn2Own) Phoenix Contact CHARX SEC-3150 DHCP Configuration Command Injection Remote Code Execution Vulnerability

ZDI-25-349	CVE-2025-5830	8.8	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial DLB_SlaveRegister Heap-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-25-348	CVE-2025-5829	6.8	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial autocharge Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-25-347	CVE-2025-5828	6.8	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial wLength Buffer Overflow Remote Code Execution Vulnerability
ZDI-25-346	CVE-2025-5827	8.8	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial ble_process_esp32_msg Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-25-345	CVE-2025-5826	6.3	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial ble_process_esp32_msg Misinterpretation of Input Vulnerability

ZDI-25-344	CVE-2025-5825	7.5	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Firmware Downgrade Remote Code Execution Vulnerability
ZDI-25-343	CVE-2025-5824	5.0	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Origin Validation Error Authentication Bypass Vulnerability
ZDI-25-342		7.5	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial PIN Missing Authentication Information Disclosure Vulnerability
ZDI-25-341	CVE-2025-5823	4.9	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Serial Number Exposed Dangerous Method Information Disclosure Vulnerability
ZDI-25-340	CVE-2025-5822	7.1	2025-06-11	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Technician API Incorrect Authorization Privilege Escalation Vulnerability

ZDI-25-330	CVE-2025-5751	4.6	2025-06-06	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger Management Card Hard-coded Credentials Authentication Bypass Vulnerability
ZDI-25-329	CVE-2025-5750	8.8	2025-06-06	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger tuya_svc_devos_activate_result_parse Heap-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-25-328	CVE-2025-5749	6.3	2025-06-06	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger BLE Encryption Keys Uninitialized Variable Authentication Bypass Vulnerability
ZDI-25-327	CVE-2025-5748	8.0	2025-06-06	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger LAN OTA Exposed Dangerous Method Remote Code Execution Vulnerability
ZDI-25-326	CVE-2025-5747	8.0	2025-06-06	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger MCU Command Parsing Misinterpretation of Input Remote Code Execution Vulnerability

2024

ZDI ID	CVE	CVSS v3.0	Published	Title
ZDI-24-1053	CVE-2024-23971	8.8	8/1/2024	(0Day) (Pwn2Own) ChargePoint Home Flex OCPP bswitch Command Injection Remote Code Execution Vulnerability
ZDI-24-1052	CVE-2024-23970	6.5	8/1/2024	(0Day) (Pwn2Own) ChargePoint Home Flex Improper Certificate Validation Vulnerability
ZDI-24-1051	CVE-2024-23969	8.8	8/1/2024	(0Day) (Pwn2Own) ChargePoint Home Flex wlanchnllst Out-Of-Bounds Write Remote Code Execution Vulnerability
ZDI-24-1050	CVE-2024-23968	8.8	8/1/2024	(0Day) (Pwn2Own) ChargePoint Home Flex
ZDI-24-1049	CVE-2024-23921	8.8	8/1/2024	0Day) (Pwn2Own) ChargePoint Home Flex wlanapp Command Injection Remote Code Execution Vulnerability
ZDI-24-1048	CVE-2024-23920	8.8	8/1/2024	(0Day) (Pwn2Own) ChargePoint Home Flex onboardee Improper Access Control Remote Code Execution Vulnerability
ZDI-24-881	CVE-2024-29206	8	6/21/2024	(Pwn2Own) Ubiquiti Networks EV Station setDebugPortEnabled Exposed Dangerous Method Remote Code Execution Vulnerability

ZDI-24-880	CVE-2024-29207	6.3	6/21/2024	(Pwn2Own) Ubiquiti Networks EV Station EVCLauncher Improper Certificate Validation Vulnerability
ZDI-24-879	CVE-2024-29208	8.8	6/21/2024	(Pwn2Own) Ubiquiti Networks EV Station changeUserPassword Missing Authentication Remote Code Execution Vulnerability
ZDI-24-873	CVE-2024-23973	8.8	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS HTTP GET Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-872	CVE-2025-2838	6.5	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS DNS Response Processing Infinite Loop Denial-of-Service Vulnerability
ZDI-24-871	CVE-2025-2837	8.8	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS HTTP Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-870	CVE-2024-24731	7.5	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS http_download Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-869	CVE-2024-23937	4.3	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS Debug Interface Format String Information Disclosure Vulnerability

ZDI-24-868	CVE-2024-23938	8.8	6/21/2024	(Pwn2Own) Silicon Labs Gecko OS Debug Interface Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-867	CVE-2024-25994	5.3	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 CharxUpdateAgent Unrestricted File Upload Remote Code Execution Vulnerability
ZDI-24-866	CVE-2024-26004	6.5	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 CANopenDevice Null Pointer Dereference Denial-of-Service Vulnerability
ZDI-24-864	CVE-2024-25998	7.5	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol UpdateFirmware Command Injection Remote Code Execution Vulnerability
ZDI-24-863	CVE-2024-26002	7.8	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 plctool Improper Privilege Management Local Privilege Escalation Vulnerability
ZDI-24-862	CVE-2024-26001	5	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 MQTT Protocol JSON Parsing Buffer Overflow Remote Code Execution Vulnerability

ZDI-24-861	CVE-2024-26005	8.8	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 ClientSession Use-After-Free Remote Code Execution Vulnerability
ZDI-24-860	CVE-2024-26003	4.3	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 HomePlug Protocol Out-Of-Bounds Read Information Disclosure Vulnerability
ZDI-24-860	CVE-2024-26003	4.3	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 HomePlug Protocol Out-Of-Bounds Read Information Disclosure Vulnerability
ZDI-24-859	CVE-2024-26000	4.3	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 MTQQ Protocol JSON Parsing Type Confusion Information Disclosure Vulnerability
ZDI-24-858	CVE-2024-26288	6.3	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Missing Encryption Authentication Bypass Vulnerability
ZDI-24-857	CVE-2024-25996	5	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Improper Access Control Firewall Bypass Vulnerability
ZDI-24-856	CVE-2024-25995	7.5	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Config Manager Improper Input Validation Remote Code Execution Vulnerability

ZDI-24-855	CVE-2024-25997	3.1	6/21/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Improper Log Output Neutralization Remote Code Execution Vulnerability
ZDI-24-854	CVE-2024-23957	8.8	6/21/2024	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 DLB_HostHeartBeat Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-853	CVE-2024-23967	8	6/21/2024	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 WebSocket Base64 Decoding Stack-based Buffer Overflow Remote Code Execution Vulnerability
ZDI-24-852	CVE-2024-23958	6.5	6/21/2024	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE Hardcoded Credentials Authentication Bypass Vulnerability
ZDI-24-851	CVE-2024-23959	8	6/21/2024	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE AppChargingControl Stack-based Buffer Overflow Remote Code Execution Vulnerability

ZDI-24-522	CVE-2024-28135	6.8	5/29/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Filename Command Injection Remote Code Execution Vulnerability
ZDI-24-521	CVE-2024-28136	7.5	5/29/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP charx_pack_logs Command Injection Remote Code Execution Vulnerability
ZDI-24-520	CVE-2024-28134	7.5	5/29/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Missing Encryption Authentication Bypass Vulnerability
ZDI-24-519	CVE-2024-28133	7.8	5/29/2024	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Untrusted Search Path Local Privilege Escalation Vulnerability

Appendix B – CWE exploited in Pwn2Own Automotive 2024/25

CWE-20: Improper Input Validation
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-120: Buffer Copy without Checking Size of Input
CWE-121: Stack-based Buffer Overflow
CWE-122: Heap-based Buffer Overflow
CWE-125: Out-of-bounds Read
CWE-134: Use of Externally-Controlled Format String
CWE-269: Improper Privilege Management
CWE-284: Improper Access Control
CWE-295: Improper Certificate Validation
CWE-306: Missing Authentication for Critical Function
CWE-321: Use of Hard-coded Cryptographic Key
CWE-345: Insufficient Verification of Data Authenticity
CWE-346: Origin Validation Error
CWE-416: Use After Free
CWE-457: Use of Uninitialized Variable
CWE-540: Inclusion of Sensitive Information in Source Code
CWE-620: Unverified Password Change
CWE-668: Exposure of Resource to Wrong Sphere
CWE-749: Exposed Dangerous Method or Function
CWE-798: Use of Hard-coded Credentials
CWE-839: Numeric Range Comparison Without Minimum Check
CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')
CWE-1191: On-Chip Debug and Test Interface with Improper Access Control
CWE-1328: Security Version Number Mutable to Older Versions

Appendix C – References

[1] https://highways.dot.gov/newsroom/investing-america-number-publicly-available-electric-vehicle-chargers-has-doubled-start

[2] Wilco van Beijnum, “Hacking EV charging stations via the charging cable”, Oct 24, 2024.

[3] Leading EV charging network hampered by Telstra outage, Jun 3, 2024.

[4] 7 Tesla Charging Stations Torched Near Boston, The New York Times, Mar 4, 2025.

[5] Gareth Corfield, “Electric car charger pulled amid warnings hackers could attack National Grid”, The Telegraph, Feb 21, 2024.

[6] Austin Dodson, “Exploitation of EV Charging System”, Southwest Research Institute, spoken at ESCAR 2022 US.

[7] Jay Johnson, “Cyberattacks and Defenses for EV Charing”, Sandia National Laboratories, spoken at ESCAR 2022 US.

[8]【江苏法治报】他一年内窃电逃费472次（02月06日A08, Feb 12, 2025.

[9] 检察日报丨堵住新能源汽车充电设备管理漏洞, Nov 30, 2018.

[10] https://x.com/klwtts/status/1619554380591824898

[11] Shamsul Aizam Zulkifli (2019), “Electric Vehicle Charging Station: Cause and Solution to Grid System”, IEEE Smart Grid.

[12] Alasali et al. (2025) “Innovative Investigation of the Resilience of EV Charging Infrastructure Under Cyber-Physical Threats Based on a Real-Time Co-Simulation Testbed”, IET Cyber-Physical Systems: Theory & Applications.

[13] “DTC P1A9096 CHECK FOR ICCU & FUSE REPLACEMENT & ICCU SOFTWARE UPDATE (RECALL 272)”, NHTSA, Nov 21, 2024.

[14] [18] Iulian Dnistran. “Hyundai’s ICCU Problem: Here’s What We Know”, Inside EVs, Mar 7, 2025.

[15] http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/e76c97207a3f332c3d55

[16] Warning over use of scam QR codes by fraudsters, East Lothian Council, Apr 25, 2025.

[17] Wu et al. (2022) “Cascading failure in coupled networks of transportation and power grid”, International Journal of Electrical Power & Energy Systems, Volume 140.

Authors

CyberThreat Research Lab, VicOne.

Task force:

Philippe Lin, Shin Li, Amadou Kane, Michael Fulgencio, Frank Domanico, William Dalton

Illuminating the Threat Landscape
of Electric Vehicle Supply Equipment
(EVSE) Infrastructure: Threat from the
Dark Web and Zero-Day Threats