VicOne | AMERICAN CENTER FOR MOBILITY
SAFE. SUSTAINABLE. SECURE.

Electric Vehicle Supply Equipment Cybersecurity:

Threat Landscape and the Road Ahead

Learn more about the partnership between VicOne, the American Center for Mobility (ACM), and Block Harbor: https://acmwillowrun.org/feature/cybersecurity/

Foreword

As the electric vehicle revolution accelerates, the infrastructure that powers it — Electric Vehicle Supply Equipment (EVSE) — is becoming a cornerstone of our energy and transportation systems. With this transformation comes a new and urgent responsibility: securing the very backbone of our mobility future.

Many in the EVSE industry have made commendable strides in aligning with cybersecurity standards. These frameworks are foundational, offering essential guidance for secure design and deployment. They provide a foundation for cybersecurity hygiene and regulatory alignment. But we must recognize that compliance is not the finish line — it is the starting point. Compliance alone is not enough.

The threats we face are not theoretical. They are real, evolving, and increasingly sophisticated. Findings from global competitions like Pwn2Own Automotive have exposed dozens of zero-day vulnerabilities in EVSE devices. These are not IT problems but are operational technology (OT) risks that directly impact the physical world: the grid, the vehicle, and the consumer.

Unlike traditional IT systems, EVSEs operate in dynamic, distributed environments. They are embedded in public spaces, connected to critical infrastructure, and often lack the hardened security layers found in enterprise networks. This makes them uniquely vulnerable — and uniquely important.

We must move beyond checkbox compliance and embrace a security-by-design mindset. That means:

- **Hardening firmware and embedded systems** against tampering and reverse engineering.
- **Securing remote update mechanisms** to prevent unauthorized code injection.
- **Implementing robust authentication and encryption** across all interfaces — wired and wireless.
- **Monitoring threat intelligence** from the clear, deep, and dark webs to stay ahead of emerging risks.
- **Collaborating across sectors** — from charge point operators (CPOs) and eMobility service providers (eMSPs) to national labs and cybersecurity firms — to build a resilient EVSE infrastructure.

This is a call to action. The EVSE industry must rise to the challenge and treat cybersecurity not as a cost center, but as a core pillar of product integrity and consumer trust. The risks are too great, and the stakes too high, to do otherwise.

Let us lead with foresight, act with urgency, and build the secure infrastructure for our future demands.

Reuben Sarkar
President & CEO, American Center for Mobility

William Dalton
VP and Managing Director (North America and Europe), VicOne

Table of Contents

Executive Summary

As electric vehicle (EV) adoption accelerates globally, the supporting infrastructure — particularly electric vehicle supply equipment (EVSE) — has become a critical component at the grid-edge and mobility ecosystems. This report, developed by VicOne in collaboration with the American Center for Mobility (ACM), provides an in-depth analysis of the evolving cybersecurity threat landscape surrounding EVSE infrastructure.

Key Findings

- **Emerging threats, not yet widespread:** While large-scale cyberattacks on EVSE have not yet materialized, numerous vulnerabilities have been uncovered through research and zero-day vulnerability contests such as Pwn2Own Automotive.
- **Pwn2Own as a bellwether:** The Pwn2Own Automotive contests revealed over 50 zero-day vulnerabilities across major EVSE brands, highlighting that many devices lack basic security protections, underscoring the urgent need for proactive mitigation.
- **Dark web and criminal activity:** Automotive threat intelligence platforms, such as VicOne's xAurient platform, have observed a growing interest among cybercriminals targeting EVSE.
- **Grid and public safety risks:** Coordinated attacks on fast-charging stations could destabilize local grids, potentially leading to blackouts and public safety hazards. Physical tampering and malware injection into chargers pose risks to both infrastructure and consumers.
- **Regulatory gaps and standards:** Compliance with standards such as ISO 15118-20, IEC 62443, and NIST IR 8473 is necessary but not sufficient. Amid an evolving threat landscape, a defense-in-depth strategy is required.

Strategic Recommendations

- **Public-private partnerships:** Collaboration among cybersecurity firms, EVSE manufacturers, charge point operators (CPOs), national labs, and federal agencies is essential to build resilient infrastructure and share threat intelligence.
- **Security by design**: EVSE manufacturers must adopt secure development practices, implement encrypted protocols, and conduct regular penetration testing and software bill of material (SBOM) analysis.
- **Threat intelligence integration**: Leveraging VicOne's xAurient and SBOM management systems, such as VicOne's xZETA, provides EVSE stakeholders with actionable and real-time insights into vulnerabilities and emerging threats across the clear, deep, and dark webs.
- **Consumer Awareness and Protection**: Education on phishing, QR code scams, and app-based fraud is vital to protect EV owners from exploitation.

While there is a relative absence of widespread attacks targeting EVSE, this should not be mistaken for security. The vulnerabilities already exist, and adversaries are watching. It is not a matter of if but when. The time for decisive action is now. Only by acting today can we safeguard the future of EVSE infrastructure.

Overview of the Current EVSE Threat Landscape

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 USA. [1] While there have been no significant observations of state-sponsored actors or advanced persistent threats (APTs) targeting EVSE to date, incidents involving ransomware, free-charging hacks, and other fraudulent activities demonstrate that vulnerabilities are already present within the EVSE infrastructure.

Cybercriminal activities: Discussions have emerged in automotive forums on whether credit card skimmers could be used at EV charging stations. However, because many e-mobility service providers (eMSPs) operate on membership-based models, it is difficult to assess the extent of consumer incidents due to the lack of publicly reported data. Documented cases remain limited, though there have been reports in China of individuals exploiting loopholes to charge EVs for free, as well as stolen credit cards used to purchase and resell home chargers for profit.

Ransomware and data breaches: In November 2024, a charging database containing personally identifiable information (PII) from various vendors and geolocations was compromised, raising concerns about data handling in EVSE-related services. At the Pwn2Own Automotive 2024 contest, researchers successfully exploited an EVSE provider that had embedded an AWS access key within a charger, exposing the risk of unauthorized access to PII and other sensitive data. While there have been no ransomware campaigns that have directly targeted EVSE to date, these incidents underscore the vulnerabilities present in current systems.

Phishing and scams: In the United Kingdom, local authorities warned consumers about fraudulent QR codes placed on charging stations. These malicious codes redirected users to fake payment portals, diverting funds away from legitimate charge point operators (CPOs). While phishing has not yet been widely observed in EVSEs, the underlying threat to consumers is evident.

Research-identified vulnerabilities: Academic research have highlighted weaknesses in charging protocols such as the Open Charge Point Protocol (OCPP) and ISO 15118, including attack vectors that can be transmitted through charging cables. [2]

Denial of service (DoS) and communication disruptions: The Telstra outage in June 2024 demonstrates the real-world impact of communication failures, as numerous ChargeFox stations ceased operation after losing connectivity with their backend charging servers. [3] Academic literature has also described DoS attacks at the protocol-level, including side-channel radio disruptions, which remain technically feasible even if not yet seen in the wild.

Insider threats: A former operations manager of a Chinese EV charging station was caught using “engineering mode” with administrator access to obtain unauthorized charging. A similar incident involved flaws in the business logic of an EV charging app that inadvertently allowed users to access charging services free of charge.

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

Grid manipulation: In the United Kingdom, sales of the Wallbox Copper SB home charger were suspended as a precautionary measure. [5] While no direct incidents have been reported or observed to date, the concerns over grid destabilization have had real impacts on businesses. Several academic studies have explored the potential for EV charging infrastructure to be leveraged in grid destabilization scenarios.

The current threat landscape for EVSE and related services is characterized by emerging and potential threats. Documented incidents so far remain limited in scale, but they already reveal weaknesses across infrastructure, protocols, and operations. As the commercial network for e-mobility continues to expand, so too will the opportunity and interest for cybercriminals to exploit vulnerabilities.

Attack Vectors in EVSE

The attack vectors targeting EVSE and its supporting infrastructure have remained largely consistent since the early research by the Sandia National Laboratories and the Southwest Research Institute. [6][7] These studies anticipated many of the vulnerabilities discovered at the Pwn2Own Automotive, the world's largest automotive zero-day vulnerability discovery contest. In both 2024 and 2025 editions of the contest, EV chargers emerged as the low-hanging fruit for security researchers, accounting for more than half of all successful exploits. Here are other key observations:

- **High exploitability.** Researchers demonstrated various vectors, including stack-based buffer overflows, unsanitized user inputs, and improperly secured services. Many of these attacks required only moderate skill, making them accessible to a wide range of adversaries.
- **Lack of basic defenses.** Several EV chargers that were exploited lacked basic security mitigations such as data execution prevention (DEP), address space layout randomization (ASLR), stack canaries, and strict input validation. This left them with a security posture comparable to consumer personal computers in the 1990s.
- **Multiple layers of exposure.** The exploited attack vectors also included physical and radio tampering with signal lines, protocol-level manipulation of programmable logic controllers (PLCs), unencrypted network connections, exposed services on LANs or WANs, and insecure firmware update mechanisms.

The following tables summarize the Common Weakness Enumerations (CWEs) observed in the Pwn2Own Automotive contest. For detailed descriptions of the CWEs, refer to Appendix B.

	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		X (WiFi SSID)			X (DHCP, PPPD)	X (API)
CWE-78		X		X (HTTP)		
CWE-120					X	
CWE-121	X		X	X		
CWE-125					X	
CWE-134				X		
CWE-269					X	
CWE-295		X				X
CWE-284		X				
CWE-416					X	
CWE-620						X
CWE-668				X (DHCP, PPPD)	X (SSH)	
CWE-798	X				X	
CWE-843					X	
CWE-1191		X				

Table 1. *CWEs exploited in EV chargers during 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-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		

Table 2. *CWEs exploited in EV chargers during Pwn2Own Automotive 2025.*

Examining the Attack Surfaces in EVSE

The attack surface of EVSE spans multiple layers, from the charging hardware and firmware running on devices to the communications protocols and backend systems that connect charging stations to broader mobility networks.

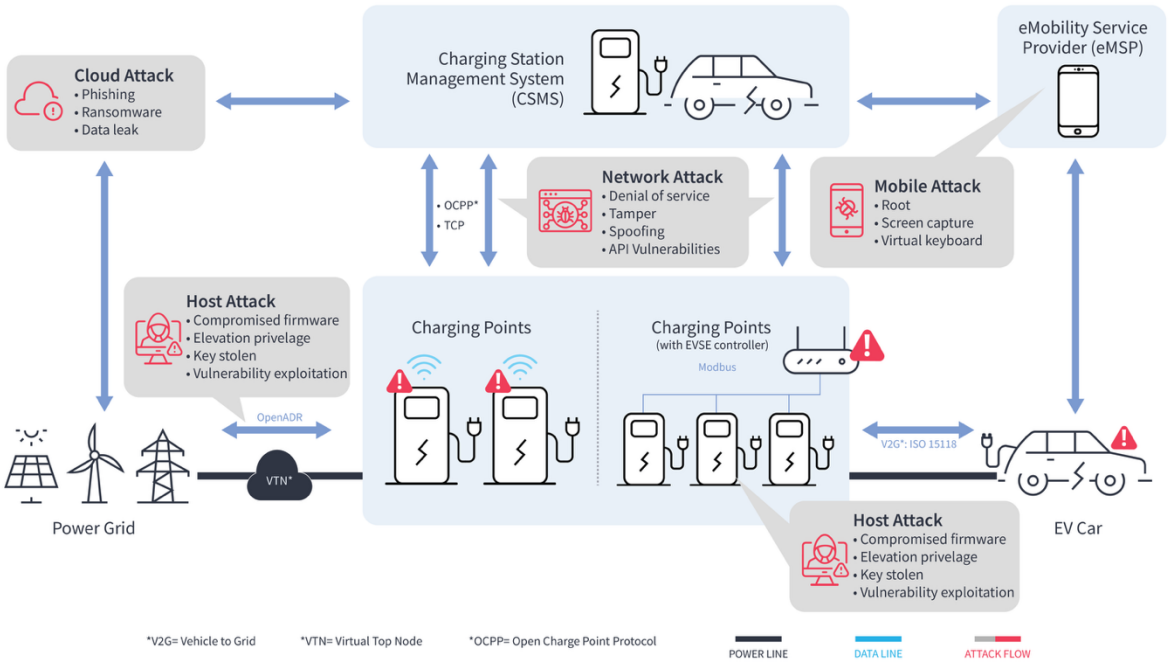

Figure 1. *Attack surfaces in EVSE span hardware, firmware, communications, backend systems, and grid interfaces.*

Here are the various attack surfaces in EVSE:

Charging hardware. Some EVSE providers ship production PCBs with debug ports, such as the JTAG still populated or accessible. This could allow attackers to connect the device to debugging tools such as the GNU Debugger (GDB), enabling them to extract the firmware, inspect the code, and modify the device's behavior.

Charging firmware and remote updates. At Pwn2Own Automotive, researchers demonstrated that over-the-air (OTA) firmware updates could be tampered with. This highlights a broader risk: if attackers can obtain or purchase an EVSE, they can almost always extract its firmware for reverse engineering and further exploitation.

Charging interfaces. EVSE interfaces, such as couplers, user terminals, backhaul connections, and maintenance ports, have been highlighted as potential attack surfaces in academic research. [7] Insider threat observations reinforce this risk, including individuals using fixed administrator PIN codes or exploiting an app with invalid logic. [8][9] One researcher even demonstrated that a radio signal could be used to jam communications on the charging cable. These cases show why charging interfaces are a critical attack surface. They are direct touchpoints between the physical charger, the user, and the broader network.

Protocol vulnerabilities. A research paper has demonstrated that protocol messages, such as the Control Pilot (CP) signal in the Combined Charging System (CCS), can be spoofed. In this case, the messages were manipulated to alter the charging current and cause DoS. [6]

Backend systems. Threats extend beyond the charger itself into eMSP backends. For example, IntelBroker claimed to have breached the Tesla charging database, sharing a sample on Breach Forums. At Pwn2Own Automotive 2024, researchers discovered a shared SSH in an EVSE device that connected back to the vendor's cloud, exposing S3 buckets containing customers' PII. Backend compromise is critical as it can cascade from a single device into large-scale consumer data exposure or operational control of charging networks.

Exposed services. Research and zero-day vulnerability contest findings continue to show that EVSE devices expose services over WAN and LAN without adequate protection. Examples include unauthenticated SSH/TelNet, vulnerable HTTP servers, and management interfaces with hardcoded credentials. The Pwn2Own Automotive contests confirmed several such cases. Exposed services matter because they expand the remote attack surface, allowing attackers to bypass access entirely.

Operating system. At the Pwn2Own Automotive contests, researchers demonstrated a wide range of operating system-level vulnerabilities in EVSE devices, including command injection over Wi-Fi SSID, configuration injection via PPPD and DHCP, JSON type confusion, insecure firewall, and multiple buffer overflows. Earlier findings also showed weaknesses in commercial products, such as JuiceBox 40's Gecko OS, which shipped with an unauthenticated Telnet server and command injection flaws. These examples highlight why the operating system is a critical attack surface. It underpins all EVSE operations, and a compromise at this layer grants attackers deep control over the device.

Unsanitized input and API entry point. At Pwn2Own Automotive 2024, one EVSE allowed password changes without validating the old password. Separately, researcher Ryan of the Kilowatts disclosed in 2023 that attackers could access Electrify America's charging stations via exposed TeamViewer sessions. [10] Such cases matter because APIs and input fields are often overlooked in security testing, yet these directly expose administrative and consumer functions to abuse.

Unsecured communications. Researchers uncovered multiple communication flaws in EVSE devices, including Bluetooth Low Energy (BLE) connections without authentication, unencrypted Bluetooth GATT traffic, TLS hostname mismatches, and SSL certificate validation failures that caused OCPP messages to be intercepted. Academic studies have also shown that some data transmitted between vehicles and chargers is unencrypted, with one case demonstrating that tapping into the charging cable provided access to internal EVSE services. [2] These examples highlight that without proper encryption and authentication, an EVSE's communication channels can be exploited to intercept or manipulate charging sessions.

Supply chain and SBOM risks. Supply chain exposure remains one of the most critical risks in EVSE, as vulnerabilities introduced through third-party hardware or software components can cascade across multiple vendors and models. While no confirmed hardware supply

chain compromises have been observed in EVSE to date, software dependency risks are already evident. VicOne's xZETA scans of firmware have uncovered outdated and vulnerable libraries in multiple devices, underscoring how software bills of materials (SBOMs) can reveal systemic weaknesses.

Grid, vehicle-to-grid (V2G), and vehicle-to-everything (V2X). As EVSE becomes more tightly integrated with the power grid, V2G and V2X interfaces represent high-value targets. Compromises at this layer could destabilize local grids, disrupting critical services. While academic studies [11] and discussions in forums have been very limited so far, the strategic importance of these interfaces makes them a critical part of the EVSE attack surface.

Beyond Compliance: Why Standards are Not Enough

The vulnerabilities discovered in Pwn2Own Automotive highlight a critical truth: standards are necessary but ultimately insufficient. While compliance frameworks exist, the contest showed that exploits can bypass protections targeting multiple layers at once, from spoofed communications to insecure operating systems and proprietary management planes. Weaknesses in firmware, update processes, and unauthenticated APIs demonstrate that adhering to a single regulatory framework or international standard will not provide adequate protection for EVSE infrastructure.

Each standard contributes important protections, but their scope is limited:

- **ISO 15118-20** defines the high-level communication (HLC) between EVs and chargers. It secures payment and data exchange using TLS encryption and Public Key Infrastructure (PKI). However, its scope does not cover the charger's operating system or administrative functions.
- **IEC 62443** treats EVSE as part of critical infrastructure, focusing on OT security. It sets requirements for firmware hardening, network segmentation, and vulnerability management.
- **ISO/SAE 21434 and UN R155** impose legal obligation on OEMs and their supply chains to implement a cybersecurity management system (CSM) and a secure software development lifecycle (SDLC) for vehicles and their components. While aimed at vehicles, these requirements also extend accountability to EVSE suppliers.
- **NIST IR 8473** integrates these elements into an actionable cybersecurity framework profile tailored for the fast-charging and EVSE infrastructure. It translates broad standards such as NIST SP 800-53r5, PCI-DSS, and IEC 62443 into a verifiable checklist mapped across four domains: EV, EVSE, cloud, and the utility grid — lowering the barrier for manufacturers to adopt a holistic security posture.

Individually, each framework has "holes," like slices of Swiss cheese — gaps where attackers can still slip through. However, when combined in a defense-in-depth approach, the layers overlap, and the holes no longer align. This is why integration, not reliance on a single standard, is essential to secure EVSE.

Insights from Threat Intelligence

Clear-Web Intelligence

The clear web refers to the publicly accessible portion of the internet, such as news sites, blogs, advisories, and academic publications that are indexed by search engines. This information is openly available, although it is often fragmented. However, recent EVSE-related stories that have surfaced illustrate both the growing interest in this domain and the real risks beginning to emerge. Notable examples include:

- **Conference research and demonstrations:** At 44CON, researchers presented "Charging Ahead," which dissected their Pwn2Own Automotive 2024 exploit of an EV charger controller. Other academic work has explored EVSE vulnerabilities through simulated charging environments, such as a real-time co-simulation testbed investigating grid resilience under cyber-physical threats. [12]
- **Protocol and software risks**: Articles have examined weaknesses in OCPP security and logic flaws in charger firmware. A critical advisory on eCharge controllers highlighted the severity of software bugs that can compromise confidentiality, integrity, and availability.
- **Vendor and vehicle incidents:** A car manufacturer issued a recall after reports of potential battery fires during fast charging, underlining how safety issues intersect with cybersecurity concerns.
- **Operational disruptions:** A Telstra outage in 2024 left EV charging networks inoperable, highlighting the importance of resilient communications for EVSE uptime.

While clear-web reports are limited and often surface-level, they serve as early warning signals for where EVSE cybersecurity issues are beginning to emerge. The VicOne threat intelligence team continues to closely monitor these developments as part of its broader research efforts.

Deep and Dark Web Intelligence

The deep web refers to online spaces not indexed by search engines, such as private forums, password-protected sites, and closed communities. The dark web is a smaller portion of this space, accessible only through specialized software, and is often associated with underground markets and criminal activity.

VicOne's threat intelligence team monitors these spaces directly and augments coverage by purchasing data from third-party providers. So far, discussions remain limited, with most activity focusing on home chargers and consumer-level issues:

- Plug-in charging concerns: Forum users raised issues about compatibility and electrical system challenges in a certain imported plug-in hybrid vehicle. Similar complaints about charging component reliability were also noted. [13][14]
- Home charger installation risks: Posts highlighted safety problems linked to improper installation of connected home charging stations, underscoring how even legitimate products can become hazardous if not deployed correctly.

- DIY vehicle conversions: A forum contributor described converting a classic 1950s luxury sedan from an internal combustion engine to an electric power source. Such modifications raise regulatory and safety concerns, particularly when conducted outside certified processes.

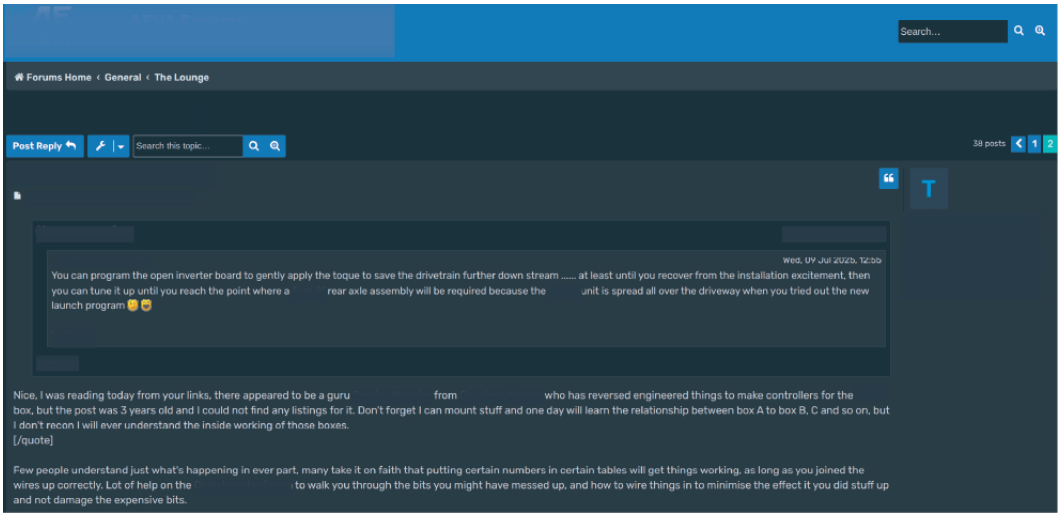

Figure 2. *Forum post regarding a DIY conversion of a classic 1950s vehicle to electric power*

The team also noted the following scattered but less credible activities:

- A carding forum user described buying and reselling home EV chargers using stolen credit cards, capitalizing on their high resale value.

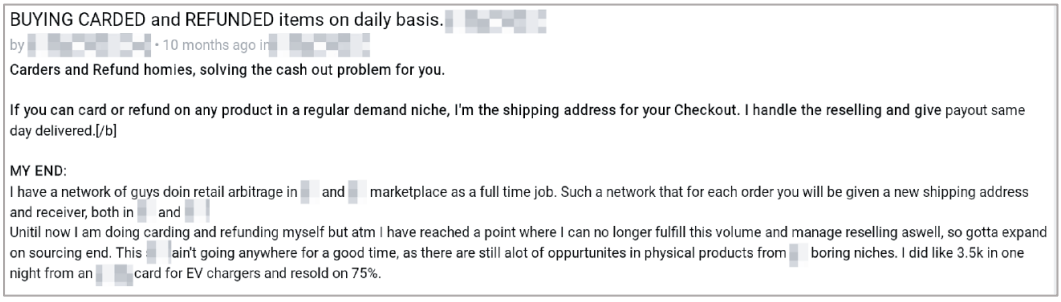

Figure 3. *A forum post on the resale of home EV chargers using stolen credit cards*

- Isolated threats to “shut down” power grids in Germany and the US, though these posts lacked technical detail and were dismissed by other forum participants. [15]

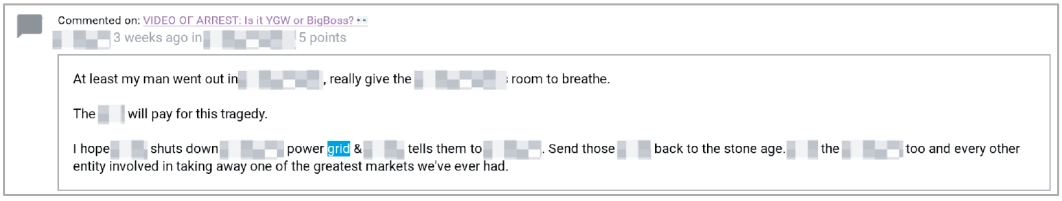

Figure 4. *A dark web post that made unsubstantiated threats to shut down national power grids*

- Ransomware monitoring revealed a July 2025 breach of a mid-sized energy services company, with stolen data later made public. While not EVSE-specific, it illustrates the broader risks energy-related companies face.

- Tender documents for a fast-charging station project were discovered in underground forums but were not retrieved due to legal reasons.

Reported EVSE-Related Incidents

In addition to monitoring the clear, deep, and dark webs, VicOne's threat intelligence team also tracks reports and claims from external sources. While not all can be independently verified, they provide insight into the types of activities and narratives emerging around EVSE security:

- **Fraudulent QR codes** (April 2025): A local government authority in the United Kingdom warned that threat actors were placing malicious QR codes on contactless payment hotspots. [16]
- **Hacktivist claims** (December 2024): The pro-Russia "Z-PENTEST ALLIANCE" allegedly claimed responsibility for attacks on an EV charging operator in South Korea. The claim was made via Telegram, but the source has since vanished.
- **Alleged data breach** (Nov 19, 2024): The actor IntelBroker posted a dataset on Breach Forums (before its shutdown in June 2025) allegedly tied to a charging management software provider. The dataset reportedly contained 116,000 rows of customer records from the Middle East, including names, locations, payment information, and vehicle identification numbers (VINs).

Figure 5. *A post with download links to alleged EVSE-related customer datasets*

These reports underscore that even unverifiable or second-hand claims can shape perceptions of EVSE security risk and emphasize the importance of continuously validating and correlating such information with other intelligence streams. VicOne's xAurient automotive threat intelligence platform supports this process by filtering the noise and delivering actionable intelligence — ensuring that EVSE industry stakeholders can prioritize real risks in an environment saturated with raw data.

The Road Ahead: Looming Threats Over EVSE

As EV adoption accelerates, charging infrastructure has become deeply integrated with national and local power grids. EV chargers, CPOs, e-MSPs, their cloud ecosystems, and connected vehicles are increasingly attracting DIY enthusiasts and curious cybercriminals. Based on observed trends and threat intelligence collected by VicOne, the EVSE cybersecurity threat landscape is expected to undergo significant evolution over the next three to five years.

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 rapid pace of technological evolution and the expansion of services make it challenging to predict the future threat landscape with precision. Still, VicOne anticipates the following several cybersecurity risks in the near term.

Unencrypted customer data, including Vehicle Identification Numbers (VINs), transaction IDs, and charging locations, could lead to data breaches and credential spoofing. Attackers may impersonate legitimate users or gain unauthorized access to EVSE services.

The emergence of **Hack-in-a-Box tools** that exploit data frame injection on charging cables and plugs may soon become widely available, giving low-tech cybercriminals new ways to tamper with EVSE systems.

Ransomware attacks could appear on EV charger displays, mirroring the ransom notes once seen on compromised ATMs. Remote EV charging stations may also serve as entry points for deeper breaches, lateral movements, and rootkit development against eMSP backends and cloud environments.

Credit card skimming and fraud may target roadside charging stations, where carders attempt to install skimmers or create fraudulent free-charging and discount apps to scam EV owners.

Physical tampering remains a concern. Criminals could unscrew station lids to inject malware or enable unauthorized charging, even selling “free-charging VIP cards.” Reverse engineering of charging apps may uncover additional pathways to exploit PII or bypass billing systems.

Nation-state activity may become more visible, moving from stealthy reconnaissance to direct disruption for both financial and political gains. Home EV chargers, which are often less maintained and less secure, could be exploited to trigger localized blackouts or cascading failures that ripple across power grids.

Grid destabilization from coordinated attacks could impact critical services such as hospitals and emergency response systems, with potentially life-threatening consequences.

Unsafe third-party components, such as unregulated charging components and chips, deteriorated integrated charging control units (ICCU), or battery management system (BMS)

units, could introduce systemic safety risks, leading to vehicle accidents, equipment failures, or even fires.

Time-synchronization exploits and novel attack techniques may emerge, targeting individual charging stations in ways not yet observed today.

Some of these risks can be effectively mitigated if EVSE manufacturers follow cybersecurity best practices. The proper implementation of encrypted protocols, regular security audits, and incident response plans will be critical in safeguarding the evolving EV charging infrastructure.

Conclusion

This report draws on recent EVSE research, VicOne's unparalleled threat intelligence across the clear, deep, and dark webs, and the analysis of zero-day vulnerabilities discovered from the Pwn2Own Automotive contests. Together, these insights lead to a clear conclusion: that EVSE risks extend beyond charging devices to the stability of the grid, public safety, and car owners. Addressing these key risks demands immediate and coordinated action.

- **Grid disruption.** Compromising multiple fast-charging stations simultaneously could destabilize the local grid, leading to voltage fluctuations, load imbalances, and frequency drift that could cascade into local or widespread blackouts. Researchers are continuously finding ways to stabilize the grids and prevent cascading failures. [17]
- **Public safety impacts.** Malicious control of chargers could disrupt charging sessions or create overcurrent conditions. Although EVs are designed with ICCUs and BMS units that disconnect in unsafe conditions, additional safeguards are crucial. This includes anti-tampering mechanisms and the replacement of vulnerable protocols, such as pulse-width modulation (PWM), to determine charging parameters.
- **Privacy and data protection.** Insecure EVSE infrastructure enables attackers to track drivers' charging locations, intercept payment data, steal credit card numbers, or interrupt vehicle charging sessions, posing both privacy violations and personal safety risks.

Securing the EVSE infrastructure requires a comprehensive defense strategy anchored in cybersecurity best practices and proactive design:

- Deploy Intrusion Detection or Prevention System (IDS/IPS), network segmentation, and hardened firewalls tailored to EVSE environments.
- Establish regular security patching, secure configuration, and remote log backups to strengthen reliance across systems.
- Leverage automotive cybersecurity platforms such as VicOne's firmware vulnerability scanning, automotive threat intelligence, and IDS/IPS solutions to stay ahead of evolving threats across the EV and charging ecosystem.

VicOne: A Key Player in End-to-End EVSE Protection

Comprehensive EVSE Protection

Automotive cybersecurity leader VicOne offers multilayered protection for EVSE manufacturers and CPOs. Our platform delivers:

- Continuous risk monitoring, real-time vulnerability discovery, and zero-day threat intelligence
- Intrusion detection and virtual patching to ensure protection even before vendor fixes are available
- SBOM analysis through xZETA, which identifies known and emerging vulnerabilities such as PerfektBlue,[18] and alerts when firmware components are at risk

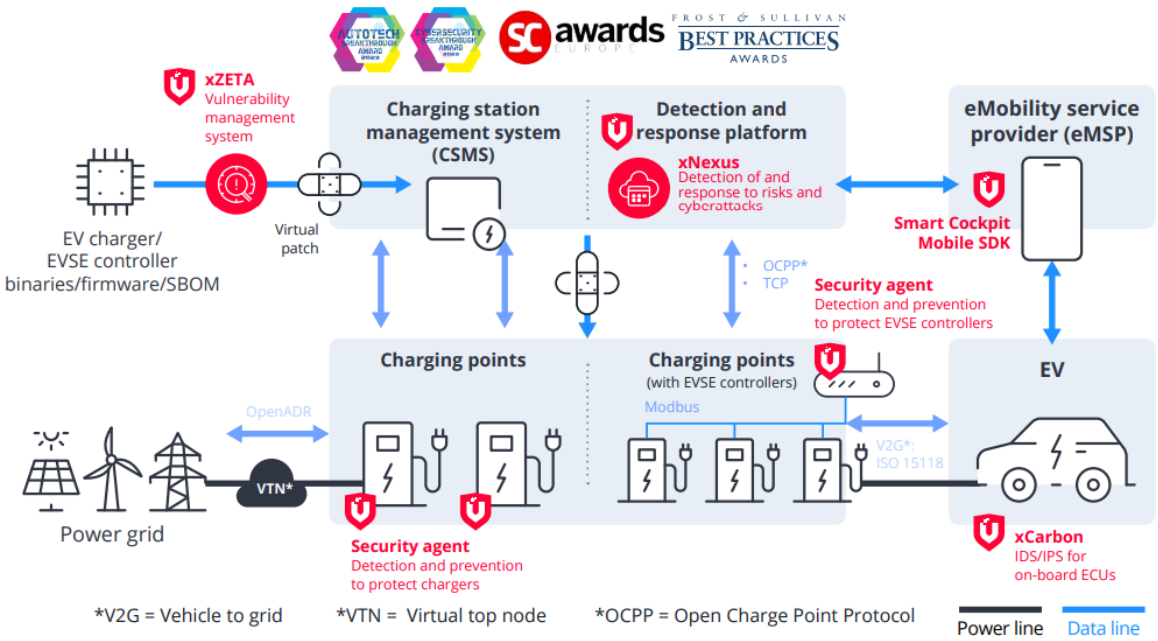

Figure 6. *VicOne's end-to-end cybersecurity solutions mapped across EVSE attack surfaces — covering hardware, firmware, communications, backend systems, and grid interfaces*

Aligned with the NIST IR 847, VicOne's award-winning solutions strengthen the four essential cybersecurity pillars: identification, detection, protection, and response — helping secure the entire EV charging lifecycle.

Applied Threat Research

VicOne's CyberThreat Research Lab continuously investigates vulnerabilities across EVSE and its related infrastructure:

- **Cellular communication risks**. Our research teams uncovered the possibility of communication spoofing through legacy 2G/3G connections in charging stations,

particularly in remote areas where insecure base stations continue to operate despite the industry's shift to LTE and 5G technologies.

- **Vendor-specific vulnerabilities and research demonstrations**. We track both vendor-specific advisories and security research. For example, the Phoenix Contact CHARX SEC-3xxx charging controller vulnerability could lead to complete compromise of confidentiality, integrity, and availability if unpatched with the recommended firmware. [19] The Tencent security team's "X-in-the-Middle Attack" demonstrated how Tesla charging ports could be opened via replay attacks on unsecured RF protocols. [20]
- **Penetration testing.** VicOne's penetration testing team conducts hands-on evaluations, such as the ongoing testing of the Emperio Level 2 EV charger, exposing vulnerabilities that are on par with and exceed those in the case of ICSA-25-196-03. [21]

Threat Intelligence Monitoring

Through the xAurient action-ready automotive threat intelligence platform, VicOne monitors the clear, deep, and dark webs for activities targeting EVSE and eMobility service providers (eMSPs). This includes:

- Breaches and vulnerabilities affecting major CPOs and eMSPs
- Carding and credit card skimming schemes directed at EV charging facilities
- Criminal resale of stolen chargers and fraudulent QR-code scams

Customers can define keywords of interest to receive immediate alerts and daily intelligence reports, enabling proactive responses to evolving threats.

Collaboration with Industry Leaders

VicOne forges strategic collaborations with industry leaders to strengthen collective defenses against the evolving EVSE and connected car landscape. These partnerships extend the benefits of advanced research, early vulnerability discovery, and shared threat intelligence across the entire EV charging ecosystem.

Through a long-standing collaboration with Trend Micro ZDI, VicOne co-hosts the Pwn2Own Automotive contests and gains early access to zero-day findings, such as Synacktiv's Tesla Wall Connector vulnerability exploit. [22]

The recent partnership with ACM underscores VicOne's commitment to building a trustworthy, end-to-end consumer charging experience. [23] By aligning our broad automotive cybersecurity solutions portfolio with their expertise, we help ensure that EVSE security keeps pace with innovation.

By combining advanced capabilities with research-driven intelligence and active collaboration, VicOne, along with ACM, ensures that EVSE security is not an afterthought but a non-negotiable foundation for the next generation of mobility.

Appendix A. CVEs Assigned to Pwn2Own Automotive Targets

2025

ZDI ID	Title	CVE	CVSS v3.0	Published
ZDI-25-712	(Pwn2Own) Tesla Wall Connector Firmware Downgrade Vulnerability	CVE-2025-8321	6.8	2025-07-29
ZDI-25-711	(Pwn2Own) Tesla Wall Connector Content-Length Header Improper Input Validation Remote Code Execution Vulnerability	CVE-2025-8320	8.8	2025-07-29
ZDI-25-628	(Pwn2Own) Phoenix Contact CHARX SEC-3150 OCPP Authentication Bypass Vulnerability	CVE-2025-25271	3.1	2025-07-22
ZDI-25-624	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Command Injection Remote Code Execution Vulnerability	CVE-2024-25995	7.5	2025-07-21
ZDI-25-623	(Pwn2Own) Phoenix Contact CHARX SEC- 3150 Origin Validation Error Firewall Bypass Vulnerability	CVE-2025-25270	6.3	2025-07-21
ZDI-25-622	(Pwn2Own) Phoenix Contact CHARX SEC-3150 Configuration Service Missing Authentication Vulnerability	CVE-2025-25268	8.8	2025-07-21
ZDI-25-621	(Pwn2Own) Phoenix Contact CHARX SEC-3150 DHCP Configuration Command Injection Remote Code Execution Vulnerability	CVE-2025-25269	8.8	2025-07-21
ZDI-25-349	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial DLB_SlaveRegister Heap- based Buffer Overflow Remote Code Execution Vulnerability	CVE-2025-5830	8.8	2025-06-11
ZDI-25-348	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial autocharge Stack-based Buffer Overflow Remote Code Execution Vulnerability	CVE-2025-5829	6.8	2025-06-11
ZDI-25-347	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial wLength Buffer Overflow Remote Code Execution Vulnerability	CVE-2025-5828	6.8	2025-06-11
ZDI-25-346	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial	CVE-2025-5827	8.8	2025-06-11

	ble_process_ esp32_msg Stack-based Buffer Overflow Remote Code Execution Vulnerability			
ZDI-25-345	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial ble_process_esp32_msg Misinterpretation of Input Vulnerability	CVE-2025-5826	6.3	2025-06-11
ZDI-25-344	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Firmware Downgrade Remote Code Execution Vulnerability	CVE-2025-5825	7.5	2025-06-11
ZDI-25-343	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Origin Validation Error Authentication Bypass Vulnerability	CVE-2025-5824	5.0	2025-06-11
ZDI-25-342	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial PIN Missing Authentication Information Disclosure Vulnerability		7.5	2025-06-11
ZDI-25-341	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Serial Number Exposed Dangerous Method Information Disclosure Vulnerability	CVE-2025-5823	4.9	2025-06-11
ZDI-25-340	(Pwn2Own) Autel MaxiCharger AC Wallbox Commercial Technician API Incorrect Authorization Privilege Escalation Vulnerability	CVE-2025-5822	7.1	2025-06-11
ZDI-25-330	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger Management Card Hard-coded Credentials Authentication Bypass Vulnerability	CVE-2025-5751	4.6	2025-06-06
ZDI-25-329	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger tuya_svc_devos_ activate_result_parse Heap-based Buffer Overflow Remote Code Execution Vulnerability	CVE-2025-5750	8.8	2025-06-06
ZDI-25-328	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger BLE Encryption Keys Uninitialized Variable Authentication Bypass Vulnerability	CVE-2025-5749	6.3	2025-06-06
ZDI-25-327	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger LAN OTA Exposed Dangerous Method Remote Code Execution Vulnerability	CVE-2025-5748	8.0	2025-06-06
ZDI-25-326	(0Day) (Pwn2Own) WOLFBOX Level 2 EV Charger MCU	CVE-2025-5747	8.0	2025-06-06

	Command Parsing Misinterpretation of Input Remote Code Execution Vulnerability			

2024

ZDI ID	Title	CVE	CVSS v3.0	Published
ZDI-24-1053	(0Day) (Pwn2Own) ChargePoint Home Flex OCPP bswitch Command Injection Remote Code Execution Vulnerability	CVE-2024-23971	8.8	8/1/2024
ZDI-24-1052	(0Day) (Pwn2Own) ChargePoint Home Flex Improper Certificate Validation Vulnerability	CVE-2024-23970	6.5	8/1/2024
ZDI-24-1051	(0Day) (Pwn2Own) ChargePoint Home Flex wlanchnllst Out-Of-Bounds Write Remote Code Execution Vulnerability	CVE-2024-23969	8.8	8/1/2024
ZDI-24-1050	(0Day) (Pwn2Own) ChargePoint Home Flex	CVE-2024-23968	8.8	8/1/2024
ZDI-24-1049	0Day) (Pwn2Own) ChargePoint Home Flex wlanapp Command Injection Remote Code Execution Vulnerability	CVE-2024-23921	8.8	8/1/2024
ZDI-24-1048	(0Day) (Pwn2Own) ChargePoint Home Flex onboardee Improper Access Control Remote Code Execution Vulnerability	CVE-2024-23920	8.8	8/1/2024
ZDI-24-881	(Pwn2Own) Ubiquiti Networks EV Station setDebugPortEnabled Exposed Dangerous Method Remote Code Execution Vulnerability	CVE-2024-29206	8	6/21/2024
ZDI-24-880	(Pwn2Own) Ubiquiti Networks EV Station EVCLauncher Improper Certificate Validation Vulnerability	CVE-2024-29207	6.3	6/21/2024
ZDI-24-879	(Pwn2Own) Ubiquiti Networks EV Station changeUserPassword Missing Authentication Remote Code Execution Vulnerability	CVE-2024-29208	8.8	6/21/2024
ZDI-24-873	(Pwn2Own) Silicon Labs Gecko OS HTTP GET Request Handling Stack- based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-23973	8.8	6/21/2024
ZDI-24-872	(Pwn2Own) Silicon Labs Gecko OS DNS Response Processing Infinite Loop Denial-of-Service Vulnerability	CVE-2025-2838	6.5	6/21/2024

ZDI-24-871	(Pwn2Own) Silicon Labs Gecko OS HTTP Request Handling Stack- based Buffer Overflow Remote Code Execution Vulnerability	CVE-2025-2837	8.8	6/21/2024
ZDI-24-870	(Pwn2Own) Silicon Labs Gecko OS http_download Stack-based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-24731	7.5	6/21/2024
ZDI-24-869	(Pwn2Own) Silicon Labs Gecko OS Debug Interface Format String Information Disclosure Vulnerability	CVE-2024-23937	4.3	6/21/2024
ZDI-24-868	(Pwn2Own) Silicon Labs Gecko OS Debug Interface Stack-based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-23938	8.8	6/21/2024
ZDI-24-867	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 CharxUpdateAgent Unrestricted File Upload Remote Code Execution Vulnerability	CVE-2024-25994	5.3	6/21/2024
ZDI-24-866	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 CANopenDevice Null Pointer Dereference Denial-of-Service Vulnerability	CVE-2024-26004	6.5	6/21/2024
ZDI-24-864	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 OCPP Protocol UpdateFirmware Command Injection Remote Code Execution Vulnerability	CVE-2024-25998	7.5	6/21/2024
ZDI-24-863	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 plctool Improper Privilege Management Local Privilege Escalation Vulnerability	CVE-2024-26002	7.8	6/21/2024
ZDI-24-862	(Pwn2Own) Phoenix Contact CHARX SEC-3100 MQTT Protocol JSON Parsing Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-26001	5	6/21/2024
ZDI-24-861	(Pwn2Own) Phoenix Contact CHARX SEC-3100 ClientSession Use-After- Free Remote Code Execution Vulnerability	CVE-2024-26005	8.8	6/21/2024
ZDI-24-860	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 HomePlug Protocol Out-Of-Bounds Read Information Disclosure Vulnerability	CVE-2024-26003	4.3	6/21/2024
ZDI-24-859	(Pwn2Own) Phoenix Contact CHARX SEC-3100 MTQQ Protocol JSON Parsing Type	CVE-2024-26000	4.3	6/21/2024

	Confusion Information Disclosure Vulnerability			
ZDI-24-858	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Missing Encryption Authentication Bypass Vulnerability	CVE-2024-26288	6.3	6/21/2024
ZDI-24-857	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 Improper Access Control Firewall Bypass Vulnerability	CVE-2024-25996	5	6/21/2024
ZDI-24-856	(Pwn2Own) Phoenix Contact CHARX SEC- 3100 Config Manager Improper Input Validation Remote Code Execution Vulnerability	CVE-2024-25995	7.5	6/21/2024
ZDI-24-855	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP Protocol Improper Log Output Neutralization Remote Code Execution Vulnerability	CVE-2024-25997	3.1	6/21/2024
ZDI-24-854	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 DLB_ HostHeartBeat Stack- based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-23957	8.8	6/21/2024
ZDI-24-853	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 WebSocket Base64 Decoding Stack- based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-23967	8	6/21/2024
ZDI-24-852	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE Hardcoded Credentials Authentication Bypass Vulnerability	CVE-2024-23958	6.5	6/21/2024
ZDI-24-851	(Pwn2Own) Autel MaxiCharger AC Elite Business C50 BLE AppChargingControl Stack-based Buffer Overflow Remote Code Execution Vulnerability	CVE-2024-23959	8	6/21/2024
ZDI-24-522	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Filename Command Injection Remote Code Execution Vulnerability	CVE-2024-28135	6.8	5/29/2024
ZDI-24-521	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP charx_pack_ logs Command Injection Remote Code Execution Vulnerability	CVE-2024-28136	7.5	5/29/2024

ZDI-24-520	(Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP charx_pack_ logs Command Injection Remote Code Execution Vulnerability	CVE-2024-28134	7.5	5/29/2024
ZDI-24-519	(Pwn2Own) Phoenix Contact CHARX SEC-3100 Untrusted Search Path Local Privilege Escalation Vulnerability	CVE-2024-28133	7.8	5/29/2024

Appendix B. CWEs Exploited in Pwn2Own Automotive

CWE	Description
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

References

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

[2] Wilco van Beijnum, https://highways.dot.gov/newsroom/investing-america-number-publicly-available-electric-vehicle-chargers-has-doubled-start

[3] CarExpert, https://www.carexpert.com.au/car-news/chargefox-ev-chargers-not-working

[4] The New York Times, https://www.nytimes.com/2025/03/04/us/politics/tesla-charging-stations-arson-boston.html

[5] The Telegraph https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/

[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, https://wxjy.jsjc.gov.cn/tslm/mtgz/202502/t20250212_1696304.shtml

[9] 检察日报, https://dx.bjjc.gov.cn/c/daxing/ajzz/308755472.jhtml

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

[11] IEEE Smart Grid, https://smartgrid.ieee.org/bulletins/march-2019/electric-vehicle-charging-station-cause-and-solution-to-grid-system

[12] Alasali, F., Ghalyon, S. A., El-Naily, N., Abuashour, M. I., AlMajali, A., Itradat, A., & Holderbaum, W. (2024). 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, 10(1), e70021. https://doi.org/10.1049/cps2.70021

[13] National Highway Traffic Safety Administration, https://static.nhtsa.gov/odi/rcl/2024/RCRIT-24V868-2647.pdf

[14] InsideEVs, https://insideevs.com/features/752768/hyundai-kia-genesis-iccu-failure/

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

[16] East Lothian Council, https://www.eastlothian.gov.uk/news/article/14501/warning_over_use_of_scam_qr_codes_by_fraudsters

[17] Fuzhang Wu, Jun Yang, Hao Jiang, Xiangpeng Zhan, Siyang Liao, Jian Xu, Hui Fan, Jifeng Liang, Cascading failure in coupled networks of transportation and power grid, International Journal of Electrical Power & Energy Systems, Volume 140, 2022, 108058, ISSN 0142-0615, https://doi.org/10.1016/j.ijepes.2022.108058

[18] PCA Cyber Security, https://perfektblue.pcacybersecurity.com/

[19] VDE CERT , https://perfektblue.pcacybersecurity.com/

[20] Black Hat Asia 2021, https://www.blackhat.com/asia-21/briefings/schedule/#x-in-the-middle-attacking-fast-charging-piles-and-electric-vehicles--22055

[21] Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/news-events/ics-advisories/icsa-25-196-03

[22] VicOne, https://vicone.com/blog/from-pwn2own-automotive-2025-unpacking-the-tesla-wall-connector-exploit-chain-and-its-broader-cybersecurity-implication

[23] VicOne, https://vicone.com/company/press-releases/american-center-for-mobility-partners-with-vicone-and-block-harbor-on-cybersecurity

Authors

Reuben Sarkar
President & CEO, American Center for Mobility
reuben.sarkar@acmwillowrun.org

William Dalton
VP and Managing Director for North America and Europe, VicOne
william_dalton@vicone.com

CyberThreat Research Lab, VicOne

EVSE Cybersecurity:
Threat Landscape and the
Road Ahead

Learn more about the partnership between VicOne, ACM, and Block Harbor:
https://acmwillowrun.org/feature/cybersecurity/