PWN2OWN AUTOMOTIVE 2026 | EXCLUSIVE INSIGHTS

Tap to Pwn

Exclusive EVSE Attack Surfaces from Pwn2Own Automotive 2026

Zia Elia
Account Executive, VicOne North America

EVSE Expansion Outpaces Cybersecurity

1 Expanding Exposure

The rapid deployment of charging ports—192,000 in the U.S. and ~34,000 in Canada—has broadened the attack surface across connected EVSE networks and backend systems.

2 Lagging Cybersecurity Maturity

Despite this growth, most EVSE operators rely on traditional IT tools that protect networks, not embedded firmware or controllers. This mismatch creates unseen vulnerabilities in the charging network.

3 Evolving Threat Activity

While no Advanced Persistent Threats (APT) or state-sponsored campaigns are evident, data and PII breaches, fraud, and vulnerabilities show that cybercriminals are increasingly probing the EV ecosystem.

VicOne

EVSE Threat Landscape

Cybercriminal activities

Ransomware and data breaches

Phishing and scams

Physical threats and vandalism

Research-identified vulnerabilities

Denial of service (DoS) and communication disruptions

Insider threats

Grid manipulation

VicOne

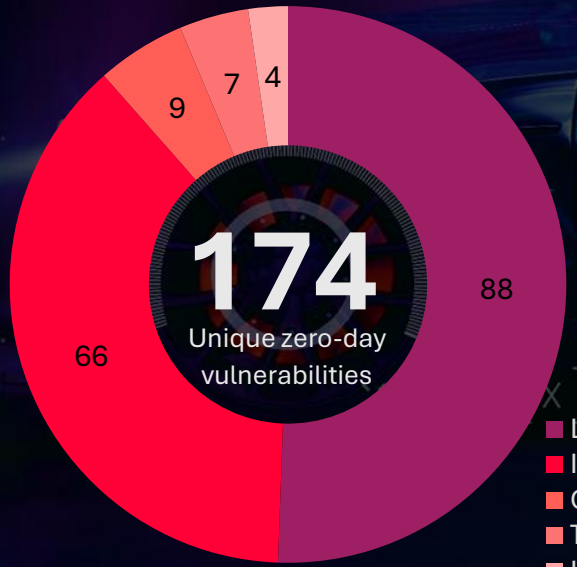
VicOne | ZERO DAY INITIATIVE

PWN2OWN AUTOMOTIVE

The world's largest zero-day vulnerability discovery contest focused on software-defined vehicles and EV Charging Infra.


AUTOMOTIV

#1 in the world to discover zero-day vulnerability



- Level 2 Electric Vehicle Chargers
- IVI systems
- OS
- Tesla
- Level 3 Electric Vehicle Chargers

TrendAI™ Zero Day Initiative™ (ZDI) Disclosed

73%

of vulnerability in the market

(Leading the way since 2007)

VicOne | ZERO DAY INITIATIVE

PWN2OWN AUTOMOTIVE

102 Days

of protection ahead of vendor patch

*Based on verified vulnerabilities from participating vendors in 2024

VicOne

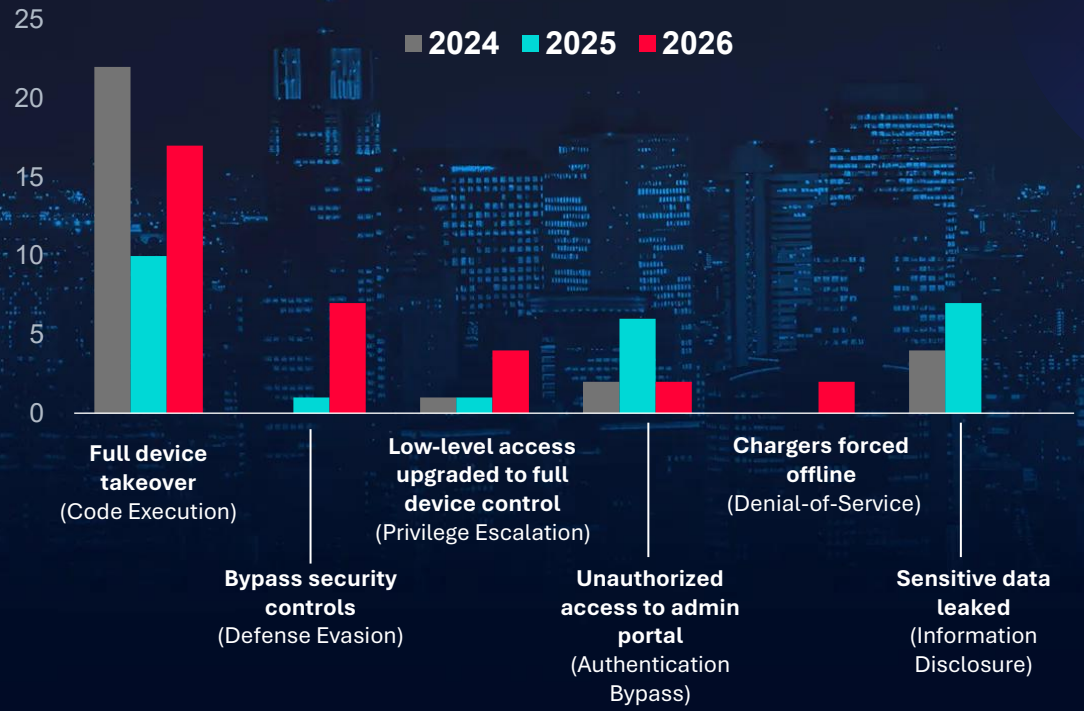
610
Total Incidents *(2024 total: 215)*

1,384
Vulnerabilities *(2024 total: 954)*

$9.4B
Cyberattack damage cost in 2025

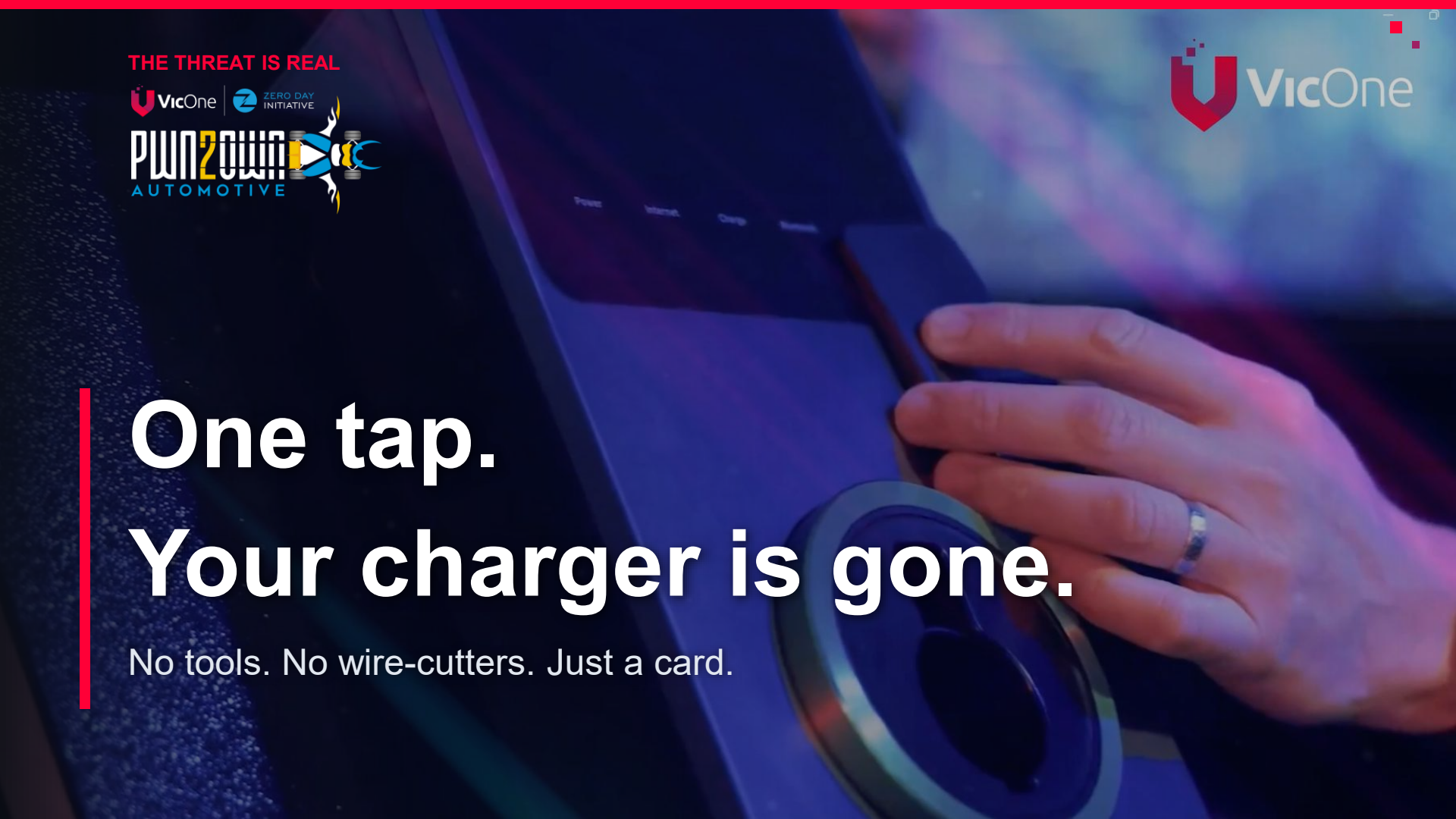
VicOne

Impact



VicOne | ZERO DAY INITIATIVE
PWN2OWN AUTOMOTIVE

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


THE THREAT IS REAL
VicOne
ZERO DAY INITIATIVE
PWN2OWN AUTOMOTIVE
VicOne
One tap.
Your charger is gone.
No tools. No wire-cutters. Just a card.

EVIDENCE #1

Free Charging for the Entire City: Authentication Bypass via NFC

HOW IT WORKS

1. Any NFC card tapped
   - No special tool
2. Charger accepts
   - No check, 4cm range
3. Exploit and granted Admin privilege
   - CWE-306: Missing Authentication
4. All chargers set free
   - Network-wide push
5. Certified product. Pwned.
   - City-scale free charging
   - One tap → mass impact

BUSINESS IMPACT

Revenue Loss

Unauthorized free charging at scale

Network Backdoor

Corp network entry via BMS integration

Mass Scale

One tap attack scales city-wide

The pattern is not an accident.

96 zero-days. All are certified, compliant products.

Pwn2Own is not a simulation. These are real devices.
The same brands are deployed across the US today.

>55%

of all Pwn2Own Automotive exploits targeted EV chargers

9

major EVSE brands attacked in 2026

THE SCALE

America is deploying 500,000 of these chargers.

192,000 ports today. 500,000 mandated by 2030. Being installed right now.


"We have ISO 15118.
We have IEC 62443.
We are secure."

COMPLIANCE VS. REALITY

What Standards Promise vs. What Pwn2Own Automotive Reveals

THE STANDARD SAYS…	PWN2OWN AUTOMOTIVE REVEALS…
ISO 15118 mandates TLS/PKI for V2G comms	V2G channel intercepted — commands spoofed in transit (CWE-345)
IEC 62443 mandates firmware hardening	Hard-coded credentials embedded in shipping firmware (CWE-798)
ISO/SAE 21434 defines automotive CSMS requirements	EVSE supply chain excluded from CSMS scope entirely
IEC 62443 requires secure authentication on all critical functions	Critical functions accessed without any authentication (CWE-306)
NIST IR 8473 mandates supply chain risk management	75 zero-days shipped to market undetected across 9 brands

Compliance is not Security.

Proven by 96 zero-days on certified products · Pwn2Own Automotive 2024–2026

IT Security ≠ Product Security

Traditional IT tools cannot identify or mitigate EVSE-specific risks (i.e., insecure firmware, EVSE-related protocol vulnerabilities, EV charger firmware vulnerabilities, supply chain risks), leaving critical gaps in compliance and safety.

IT Security

focuses on protecting networks, endpoints, and user access.

IT Security Examples:

- Firewalls, SIEM alerts, and VPNs
- Protecting cloud infra and backend servers

Product Security

ensures that physical systems remain secure throughout their lifecycle.

Product Security Examples:

- Firmware vulnerability discovery and triage
- 3rd party supply chain SBOM/HBOM correlation
- OCPP security event correction
- Host-based IDPS

THE PATH FORWARD

Beyond compliance. Toward real security.

The tools that see what standards can't.

- xAurient threat intelligence: clear, deep and dark web monitoring for EVSE-targeted attacks
- xZETA product security platform: find vulnerable libraries in your charger firmware before attackers do
- Pwn2Own Automotive: Exclusive zero-day intelligence, 102 days before any vendor patch exists

The path forward is product-level security, not compliance alone

VicOne

Compliance Is the Starting Line.
Security Is the Finish.

VicOne turns exclusive Pwn2Own Automotive zero-day intelligence into real protection for your EVSE network.

Talk to a VicOne Expert