


Malware & Threats ▾ Security Operations ▾ Security Architecture ▾ Risk Management ▾

DEVO

EBOOK CISO Strategy ▾ ICS/OT ▾ Funding/M&A ▾

Journey to the Autonomous SOC

Download Now



aws Available in AWS Marketplace

IOT SECURITY

EV Charging Management System Vulnerabilities Allow Disruption, Energy Theft

Vulnerabilities in electric vehicle charging management systems can be exploited for DoS attacks and to steal energy or sensitive information.



By [Eduard Kovacs](#)
February 2, 2023



Researchers warn that many electric vehicle (EV) charging management systems are affected by vulnerabilities

TRENDING

The Effect of Cybersecurity Layoffs on Cybersecurity Recruitment

Zendesk Hacked After Employees Fall for Phishing Attack

Russia-Linked APT29 Uses New Malware in Embassy Attacks

Microsoft Urges Customers to Patch Exchange Servers

that could allow hackers to cause disruption, steal energy, or obtain driver information.

The vulnerabilities were discovered by researchers working for SaiFlow, an Israel-based company that specializes in protecting EV charging infrastructure and distributed energy resources.

The security holes are related to the communications between the charging system management service (CSMS) and the EV charge point (CP), specifically the use of the Open Charge Port Protocol (OCPP). The flaws have been confirmed to impact the CSMS offered by multiple vendors.

The problem is related to the use of WebSocket communications by the OCPP and how it mishandles multiple connections. The protocol does not know how to handle more than one CP connection at a time and attackers could abuse this by opening a new connection to the CSMS. Another issue is related to what SaiFlow describes as "weak OCPP authentication and chargers identities policy".

By opening a new connection to the CSMS on behalf of a charge point, the attacker causes the original connection to be closed or to become nonfunctional.

According to SaiFlow, an attacker can exploit the weaknesses to launch a distributed denial-of-service (DDoS) attack that disrupts the electric vehicle supply equipment (EVSE) network. In addition, if an attacker can connect to the CSMS, they

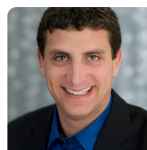
Cyberattacks Target Websites of German Airports, Admin

Critical Vulnerability Impacts Over 120 Lexmark Printers

Meta Awards \$27,000 Bounty for 2FA Bypass Vulnerability

US Infiltrates Big Ransomware Gang: 'We Hacked the Hackers'

EXPERT INSIGHTS



Dealing With the Carcinization of Security

Varied viewpoints as related security concepts take on similar traits create substantial confusion among security teams

may be able to obtain drivers' personal information, including payment card data, as well as other sensitive data, such as server credentials.

In certain configurations, if the charger approves unknown driver identities, an attacker may be able to charge their vehicle without paying for it, the security firm said.

"Since the CSMS platforms are publicly accessible, it is possible for an attacker to hijack the connection remotely, without needing to gain credentials, access, or perform MITM attacks," Ron Tiberg-Shachar, co-founder and CEO of SaiFlow, told *SecurityWeek*.

Tiberg-Shachar believes it may be possible for a somewhat inexperienced hacker to carry out an attack, even with limited resources.

In order to conduct an attack, the hacker first needs to obtain a charger's identity. This identity typically has a standard structure, making it easier for threat actors to enumerate the values of valid identifiers.

In the next phase, they need to obtain information on which CSMS platform the charger is connected to. The expert noted that the CSMS URL can be discovered using services such as Shodan or SecurityTrails.

SaiFlow has published a technical blog post [describing the vulnerabilities and the attack scenarios](#). The company also

trying to evaluate and purchase security technologies.

Marc Solomon



Stop, Collaborate and Listen: Disrupting Cybercrime Networks Requires Private-Public Cooperation and Information Sharing

No one combatting cybercrime knows everything, but everyone in the battle has some intelligence to contribute to the larger knowledge base.

Derek Manky



How the Atomized Network Changed Enterprise Protection

Our networks have become atomized which, for starters, means they're highly dispersed. Not just in terms of the infrastructure – legacy, on-premises, hybrid, multi-cloud, and edge.

Matt Wilson



Mapping Threat Intelligence to the NIST Compliance Framework Part 2

How threat intelligence is critical when justifying budget for GRC personnel, and for threat intelligence, incident response, security operations and CISO buyers.

Landon Winkelvoss



Password Dependency: How to Break the Cycle

Hackers rarely hack in anymore. They log in using stolen, weak, default, or otherwise compromised credentials. That's why it's so critical to break the password dependency cycle. But how can this be done?

Torsten George

provides recommendations for how these types of attacks can be mitigated.

It doesn't seem like the vulnerabilities can be easily patched by vendors.

"We've approached many key players in the industry (and keep on doing so) to make them aware of our findings and how they can approach a solution," Tiberg-Shachar said. "Additionally, we've made our solutions team available to support any specific technical questions, in an effort to reinforce vulnerabilities as quickly as possible. Our key goal is to support partners in scaling their charging infrastructure as quickly and safely as possible."

Related: [Unpatched Econolite Traffic Controller Vulnerabilities Allow Remote Hacking](#)

Related: [Remote 'Brokenwire' Hack Prevents Charging of Electric Vehicles](#)

Related: [New Flaws Expose EVlink Electric Vehicle Charging Stations to Remote Hacking](#)

LATEST NEWS

Zendesk Hacked After Employees Fall for Phishing Attack

Malicious Prompt Engineering With ChatGPT

Cyberattacks Target Websites of German Airports, Admin

GoTo Says Hackers Stole Encrypted Backups, MFA Settings

NSA Publishes Security Guidance for Organizations Transitioning to IPv6

WRITTEN BY

Eduard Kovacs

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard

