EV ŞARJ İSTASYONU GÜVENLİĞİ SWOT ANALİZİ

Hazırlanma Tarihi: 11 Kasım 2025

Belge Amacı: Elektrikli araç (EV) şarj istasyonu (EVSE) altyapısının, gelişmiş siber tehditler (Yapay Zeka destekli zafiyet taraması, SSRF) ve dahili protokol (CAN bus) zayıflıkları karşısındaki güvenlik duruşunu analiz etmek.

GÜÇLÜ YÖNLER (STRENGTHS)

(Sistemin mevcut içsel avantajları ve savunma mekanizmaları)

- **Protokol Olgunlaşması (OCPP 2.0.1):** OCPP 2.0.1 ve ISO 15118 gibi yeni nesil protokoller, "tasarımdan güvenli" (secure-by-design) bir yaklaşım benimser. Zorunlu TLS, PKI (Açık Anahtar Altyapısı) ve cihaz sertifikaları, SSRF gibi saldırılar için kritik olan yetkisiz ağ erişimini ve sahteciliği (spoofing) önemli ölçüde zorlaştırır.
- **Fiziksel İzolasyon (CAN Bus):** CAN bus, doğası gereği harici IP ağlarından (İnternet) izole bir protokoldür. Bir saldırganın CAN bus'a doğrudan uzaktan erişmesi için öncelikle istasyonun IP ağına (örn. bir SSRF zafiyeti yoluyla) sızması ve ardından bir ağ geçidini (gateway) aşması gerekir.
- **Savunma için AI Kullanımı:** Saldırganların AI kullanması bir tehdit iken, savunma tarafının da AI kullanması bir güçtür. AI destekli Davranışsal Analiz (UEBA) ve Anomali Tespiti sistemleri, "normal" CAN bus veya OCPP trafik modellerinin dışına çıkan AI kaynaklı gelişmiş fuzzing saldırılarını tespit etme potansiyeline sahiptir.
- **Merkezi Yönetim (CSMS):** Güvenli bir şekilde yapılandırılmış bir CSMS (Merkezi Yönetim Sistemi), istasyonlardaki anormallikleri (örn. bir SSRF saldırı girişimi veya beklenmedik CAN hata çerçeveleri) merkezi olarak izleyebilir, günlüğe kaydedebilir ve şüpheli istasyonları hızla devre dışı bırakabilir (karantinaya alabilir).

ZAYIF YÖNLER (WEAKNESSES)

(Sistemin mevcut içsel kusurları ve protokol zafiyetleri)

- **CAN Bus Protokolünün Mirası:** CAN bus, kimlik doğrulama, şifreleme veya kaynak doğrulama mekanizmalarından yoksundur. Ağa erişim sağlandığı anda (örn. bir SSRF ile aşılan bir pivot noktası aracılığıyla), tüm düğümler (ECU'lar) "güvenilir" kabul edilir. Bu, enjeksiyon (injection) ve sahtecilik (spoofing) saldırılarını önemsiz hale getirir.
- **Yetersiz Giriş Doğrulaması (SSRF Kök Nedeni):** Birçok EVSE ve CSMS web arayüzü veya API uç noktası, kullanıcıdan alınan girdileri (örn. URL, IP adresi) yeterince temizlemez veya doğrulamadan işler. Bir "tanılama pingi", "firmware güncelleme URL'si" veya "rapor sunucusu" gibi işlevler, SSRF saldırıları için birincil giriş noktalarıdır.
- **Düz (Flat) Ağ Mimarisi:** Birçok şarj istasyonunun dahili mimarisi, harici iletişim modülünü (LTE/Ethernet), web sunucusunu ve CAN bus ağ geçidini aynı mantıksal ağ üzerinde tutar. Güvenlik duvarı veya segmentasyon eksikliği, başarılı bir SSRF saldırısının doğrudan CAN ağ geçidine (gateway) pivot yapmasına olanak tanır.
- **Eski Protokol Yükü (OCPP 1.6):** Sahadaki istasyonların büyük çoğunluğunun hala zorunlu şifreleme (Güvenlik Profili 1) kullanmayan OCPP 1.6'yı kullanması, AI destekli araçların ağ trafiğini dinleyerek (sniffing) sistem mimarisini ve potansiyel SSRF hedeflerini öğrenmesini kolaylaştırır.

FIRSATLAR (OPPORTUNITIES)

(Güvenlik duruşunu iyileştirmek için kullanılabilecek dışsal etkenler)

- **Sıfır Güven Mimarisi (Zero Trust Architecture - ZTA):** SSRF ve AI gibi gelişmiş tehditler, "güven ama doğrula" modelinin yetersizliğini kanıtlamıştır. ZTA'nın benimsenmesi (örn. her dahili bileşenin birbiriyle iletişim kurmak için bile sertifika kullanması), bir SSRF saldırısının yanal hareket (lateral movement) kabiliyetini büyük ölçüde kısıtlar.
- **CAN Bus için Eklenti Güvenliği:** CAN bus protokolü güvensiz olsa da, üzerine güvenlik katmanları eklenebilir. CANsec (şifreleme ekler), CAN IDS/IPS (anomali tespiti) ve CAN ağ geçidi güvenlik duvarları (yalnızca izin verilen ID'lere izin veren) gibi teknolojiler için pazar ve talep artmaktadır.
- **Yasal Düzenlemeler (CRA, PSTI):** AB Siber Dayanıklılık Yasası (CRA) gibi yeni düzenlemeler, üreticileri "tasarımdan güvenli" ürünler yaratmaya ve bilinen zafiyetler (SSRF gibi) için yamalar sağlamaya yasal olarak zorlamaktadır. Bu durum, endüstri genelinde güvenlik seviyesini yükseltecektir.
- **AI Odaklı Güvenlik Testleri (Pentest):** Şirketlerin, saldırganlardan önce davranarak kendi sistemlerini AI destekli fuzzing ve otonom sızma testi araçlarıyla test etmesi, özellikle karmaşık protokollerdeki (CAN, ISO 15118) mantık hatalarını ve SSRF zafiyetlerini proaktif olarak bulmalarını sağlar.

TEHDİTLER (THREATS)

(Sistemin kontrolü dışındaki dışsal riskler ve aktörler)

- **AI Destekli Fuzzing ve Zafiyet Keşfi:** En büyük tehdittir. Yapay zeka modelleri, CAN bus veya OCPP gibi durum bilgisi olan (stateful) protokollerin "normal" davranışını öğrenebilir. Geleneksel fuzzer'ların aksine, AI, sistemin çökmesine neden olmayacak ancak onu istenmeyen bir duruma (örn. ücretsiz şarj) sokacak veya güvenlik kontrollerini atlatacak (örn. SSRF filtreleri) son derece karmaşık ve hedefe yönelik mesaj dizileri üretebilir.
- **SSRF'in CAN Bus'a Pivot Vektörü Olarak Kullanılması:** Bu, en tehlikeli saldırı senaryosudur
    1. **Aşama 1 (Dış):** Saldırgan, istasyonun web arayüzünde veya CSMS'nin bir API'sinde bir SSRF zafiyeti bulur.
    2. **Aşama 2 (İç):** Saldırgan, bu zafiyeti kullanarak istasyonun *iç ağına* (örn. `http://192.168.1.5/can_gateway_admin`) istekler gönderir.
    3. **Aşama 3 (Pivot):** Saldırgan, CAN ağ geçidinin (gateway) yönetici arayüzünü (eğer zayıf parolalıysa) ele geçirir veya doğrudan ağ geçidi aracılığıyla ham CAN mesajları enjekte etmenin bir yolunu bulur.
- **AI ile Güçlendirilmiş SSRF:** Saldırganlar, WAF (Web Application Firewall) veya filtreleri atlatmak için AI kullanarak SSRF payload'larını (örn. IP adresi kodlaması, farklı protokoller kullanma `gopher://`, `file:///`) sürekli olarak değiştiren ve obfuskasyon (gizleme) yapan araçlar geliştirebilir.
- **Geniş Ölçekli Şebeke Saldırıları (Grid Destabilization):** CAN bus veya SSRF yoluyla ele geçirilen binlerce istasyondan oluşan bir botnet, AI tarafından koordine edilerek (örn. talebin en yüksek olduğu anda eşzamanlı olarak şarjı kesmek veya başlatmak), bölgesel elektrik şebekesinde ciddi istikrarsızlığa yol açabilir.

STRATEJİK ÇIKARIM VE ÖNCELİKLİ EYLEM PLANI

Bu analiz, **SSRF zafiyetlerinin artık yalnızca bir web zafiyeti olmadığını**, EV şarj altyapısı bağlamında **siber-fiziksel bir tehdit** haline geldiğini göstermektedir. SSRF, IP tabanlı ağlar (İnternet/OCPP) ile araç içi kontrol ağları (CAN bus) arasındaki kritik "köprü" görevi görebilir.

Yapay zeka, bu saldırıları hem keşfetme (fuzzing) hem de yürütme (filtre atlatma) açısından hızlandırmaktadır.

Acil Eylem Planı:

1. **Dahili Ağ Segmentasyonu:** Tüm EVSE tasarımlarında, harici iletişim modülü, web sunucusu ve CAN bus ağ geçidi **mutlaka** katı güvenlik duvarı kurallarıyla birbirinden ayrılmalıdır.

2. **Giriş Doğrulama ve İzin Listesi (Allow-Listing):** SSRF'i önlemek için, dışarıdan alınan tüm URL/IP girdileri katı bir "izin listesine" (allow-list) tabi tutulmalı, diğer tüm istekler reddedilmelidir.
3. **CAN Ağ Geçidi (Gateway) Güvenliği:** CAN ağ geçidi, yalnızca önceden tanımlanmış, güvenli komutları (örn. "şarjı başlat") kabul etmeli, ham veya keyfi CAN mesajlarının IP ağından enjekte edilmesini engellemelidir.

Sacide Aişenur Direk