# Anomali Senaryosu Raporu

## Senaryo Adı: OCPP Komut Spam'i ve "Uykucu Şarj Cihazı" – Hizmet Reddi (DoS)

### Hazırlayan

Muhammed KARTAL

### Tarih

30.10.2025

## 1. Senaryonun Amacı

Bu raporun amacı, OCPP protokollü elektrikli araç şarj istasyonlarında meydana gelebilecek bir DoS anomalisini teknik ve operasyonel açıdan detaylandırmaktır. Senaryo, hem ağ seviyesi flooding hem de mantıksal/iş mantığı-odaklı komut spam'i (ör. SetChargingProfile suistimali) yollarıyla hizmetin reddedilmesini kapsamaktadır.

## 2. Senaryo Özeti

Saldırganın hedefi, kullanıcıların şarj hizmetine erişimini engelleyerek operasyonel aksama ve maddi zarar üretmektir. Saldırgan, ele geçirilmiş CSMS kimlik bilgileri ya da MitM konumu kullanarak hedef istasyonlara aşırı sayıda OCPP komutu gönderir ve/veya SetChargingProfile ile akımı 0A yapan ve uzun süreli parametreler içeren profiller uygulayarak istasyonların fiziksel enerji vermesini engeller.

## 3. Hedef Varlıklar

- Charge Point Controller (CP Ana Denetleyicisi)  
- CSMS yönetim panosu ve API uç noktaları  
- Kullanıcı deneyimi (mobil uygulama / kiosk)  
- Fiziksel şarj altyapısı (röleler, güç elektroniği)

## 4. STRIDE Sınıflandırması

Denial of Service (DoS) – birincil  
Ayrıca: Tampering (profil parametrelerinin manipülasyonu), Repudiation (logların manipülasyonu ile tespit zorluğu)

## 5. Zafiyetler

1. CSMS hesap güvenliğinin zayıf olması (MFA yok, zayıf parolalar, uzun süreli API anahtarları).  
2. ChargingProfile parametre doğrulamasının yetersiz olması (min/max current, duration limitleri).  
3. Rate limiting ve circuit-breaker mekanizmalarının eksik veya yanlış konfigüre edilmiş olması.  
4. Yetersiz telemetri ve log korelasyonu (Heartbeat/MeterValues/energy meter mismatch).  
5. Log ve diagnostic upload kontrollerinin yetersiz olması (repudiation riski).

## 6. Saldırı Adımları (Detaylı)

Aşama A: Hazırlık ve Erişim

1. Hedef seçimi: Operatörün en yaygın ve en zayıf güvenlik uygulayan CSMS veya istasyon filosu seçilir.  
2. İlk erişim: Phishing, zayıf yama yönetimi veya açık API zafiyetiyle CSMS yönetici hesabı ele geçirilir veya MitM konumu sağlanır.

Aşama B: Deneme ve İnce Ayar

1. Saldırgan, küçük ölçekli komut spam'leri ile istasyonların davranış sınırlarını keşfeder.  
2. ChargingProfile yüklemeleriyle hangi parametrelerin kabul edildiği test edilir (ör. duration, min/max current).  
3. Loglama/teşhis süreçlerini kontrol ederek tespit olasılığını azaltacak yöntemler belirlenir.

Aşama C: Tetikleme ve Sürdürme

1. Büyük ölçekli komut gönderimi başlatılır: RemoteStart/Stop veya SetChargingProfile komutları yüksek frekansta gönderilir.  
2. Uykucu istasyon yöntemi: SetChargingProfile ile current=0A ve duration çok uzun (örn. 10 yıl) uygulanır.  
3. Saldırgan periyodik olarak profili yeniden uygular veya CSMS hesabı üzerinden yeniden yapılandırma yaparak istasyonu hizmet dışı tutar.

## 7. Etkiler

- Kullanıcılar istasyonlarda şarj yapamaz; müşteri şikayetleri artar.  
- Operasyonel gelir kaybı ve potansiyel tazminat talepleri.  
- Operatör, istasyonları fiziksel olarak kontrol etmek için maliyetli saha ziyaretleri yapabilir.  
- Uzun süre devam eden saldırılar, marka güvenini ve kamu güvenini zedeler.  
- Kritik altyapı işletmelerinde (lojistik filoları vb.) ciddi hizmet aksaklıkları oluşabilir.

## 8. Tespit Yöntemleri (Detaylı)

A. Kural Tabanlı İzleme  
 - OCPP mesaj frekansı eşiği (ör. saniyede X komuttan fazla) ve aynı CSMS-Account/ChargePoint ilişkisinde anormallik tespiti.  
 - ChargingProfile parametrelerinin beklenen aralığın dışındaysa otomatik reddetme ve uyarı.  
B. Telemetri Korelasyonu  
 - Heartbeat/MeterValues vs fiziksel enerji sayacı verisi (smart meter) karşılaştırması.  
 - Eğer MeterValues raporları enerji akışı göstermiyorsa ama oturum aktif görünüyorsa anomali.  
C. ML/İstatistiksel Yöntemler  
 - Zaman serisi modelleri (seasonal decomposition) ile normalin dışındaki komut yoğunluğu tespiti.  
 - Isolation Forest veya One-Class SVM ile nokta anomalileri.  
D. Adli İzleme ve Log Bütünlüğü  
 - Logların kriptografik imza/append-only yapı ile korunması; upload erişimlerinin sınırlandırılması.

## 9. Önleme ve Azaltma Stratejileri (Detaylı)

1. Kimlik ve Erişim Yönetimi  
 - CSMS hesapları için zorunlu MFA, kısa ömürlü API anahtarları, düzenli anahtar rotasyonu.  
2. Input Doğrulama ve Politikalar  
 - ChargingProfile için işletimsel limitler (max duration, min/max current) ve server-side validation.  
3. Rate Limiting ve Circuit Breaker  
 - Per-CSMS-account ve per-ChargePoint rate limitler; kısa süreli aşırı yükte otomatik devre dışı bırakma ve rollback.  
4. Telemetri Çapraz Doğrulama  
 - MeterValues ile fiziksel sayaç (smart meter) doğrulaması; anormal durumlarda otomatik bilet (ticket) açma.  
5. İzleme ve Olay Müdahalesi  
 - SIEM entegrasyonu, playbook'lar; hızlı ClearChargingProfile/remote-reset komutlarıyla iyileştirme.  
6. Log Güvenliği  
 - Logların append-only, şifreli ve erişim kontrollü saklanması; kritik değişikliklerin ikinci bir onay mekanizması.  
7. Güvenlik Testleri  
 - Düzenli pentest, red-team ve CSMS güvenlik taramaları; 3. taraf bağımsız denetimler.

## 10. Örnek Algoritma: Basit Kural Tabanlı Tespit (Pseudo)

Kural:  
 - Eğer herhangi bir ChargePoint üzerinde 5 saniye içinde 10'dan fazla RemoteStart/Stop/SetChargingProfile komutu alınırsa uyarı üret.  
 - Eğer bir ChargePoint için aktif bir chargingProfile var ve MeterValues enerji akışı=0 ise otomatik uyarı ve geçici izolasyon.

## 11. Sonuç ve Öneriler

OCPP tabanlı DoS anomalisleri, hem ağ düzeyinde hem de iş mantığı seviyesinde ortaya çıkabilir. En etkin savunma, birden fazla katmanda (kimlik yönetimi, doğrulama, rate limiting, telemetri korelasyonu ve hızlı müdahale playbook'ları) kurulan savunma-in-depth stratejisidir. Operatörlerin CSMS güvenliğini sağlamak, chargingProfile doğrulaması uygulamak ve telemetriyi fiziksel sayaçlarla çapraz doğrulamak öncelikli adımlar olmalıdır.