# DOS-XX: OCPP Tabanlı DoS Anomalisi - Komut Spam ve SetChargingProfile Suistimali

## Senaryo Kodu

DOS-XX

## Senaryo Adı

OCPP Komut Spam'i ve Uykucu Şarj Cihazı Anomalisi

## Birincil Hedef

Şarj İstasyonu Denetleyicisi (Charge Point Controller), CSMS operasyonu, kullanıcı erişimi

## Anahtar Protokol(ler)

OCPP 1.6 / OCPP 2.0.1, TLS, HTTP/S

## STRIDE Kategorisi

Denial of Service (DoS)

## Tehdit Aktörü Profili

Siber suçlu, iç tehdit veya ele geçirilmiş CSMS hesabı

## Etki Şiddeti

Yüksek - Kullanıcı erişiminin kısıtlanması, operasyonel gelir kaybı, güven kaybı

## Senaryo Özeti

Saldırgan, ele geçirilmiş bir CSMS hesabı veya MitM konumu aracılığıyla hedef şarj istasyonlarına aşırı miktarda OCPP komutu (ör. RemoteStartTransaction, RemoteStopTransaction, SetChargingProfile) gönderir veya SetChargingProfile ile limitleri 0A ve uzun süreli süreler ayarlayarak cihazın fiziksel enerji sağlamasını engeller. İstasyonlar 'çevrimiçi' görünse de araçlara enerji sağlamaz; sonuç gizli, tespit edilmesi zor ve kalıcı hizmet kesintisidir.

## Temel Zafiyetler

- Yetersiz giriş/doğrulama (CSMS hesaplarına zayıf kimlik bilgileri veya el değiştirmiş API anahtarları).  
- Profil parametrelerine (chargingSchedule) yeterli doğrulama uygulanmaması.  
- Rate limiting ve circuit-breaker gibi korunma mekanizmalarının eksikliği.  
- Loglama ve telemetri alarm eşiklerinin yanlış yapılandırılması.

## Tipik Saldırı Akışı (kısa)

1. Saldırgan CSMS yönetici hesabını ele geçirir veya MitM pozisyonu elde eder.  
2. Hedef istasyonlara ardışık RemoteStart/Stop veya SetChargingProfile komutları gönderir.  
3. SetChargingProfile ile limit 0A ve uzun duration uygulanır (uykucu istasyon).  
4. Operatörler alarm/monitoring panellerinde istasyonları 'Available' görür ama araç şarj edilemez.  
5. Saldırgan periyodik olarak profili yeniden uygulayarak kesintiyi sürdürür.

## Tespit Yöntemleri (kısa)

- Komut-frekansı bazlı eşik uyarıları (ör. saniyede gelen OCPP komutları).  
- ChargingProfile parametrelerinin anomalik değerlerini otomatik reddetme/ispatlama.  
- Telemetri kıyaslama: Heartbeat, MeterValues ve gerçek enerji akışı arasındaki tutarsızlık tespiti.  
- ML tabanlı anomali tespiti: komut frekansı, yanıt süreleri, CPU/RAM spike'leri.

## Önleme/Öneriler (kısa)

- Zorunlu rate-limiting ve per-IP/ per-CSMS-account limitler.  
- ChargingProfile input doğrulaması (maksimum izin verilen duration, min/max current).  
- Circuit breakers ve otomatik rollback mekanizmaları.  
- Güç ve telemetri çapraz doğrulaması: MeterValues ile fiziksel enerji ölçer doğrulaması.  
- Merkezi CSMS için çok faktörlü kimlik doğrulama ve API anahtarı rotasyonu.