OCPP OTURUM BİLGİLERİNİN ELE GEÇİRİLMESİ SWOT ANALİZ RAPORU

OCPP (Open Charge Point Protocol), elektrikli araç şarj istasyonları ile merkezi yönetim sistemleri arasındaki iletişimi standartlaştırmak için kullanılan açık bir protokoldür.
Bu protokolde, **oturum kimliklerinin (session tokens, credentials, veya ID'ler)** kötü niyetli kişilerce ele geçirilmesi, sistem güvenliği ve kullanıcı gizliliği açısından kritik bir zafiyet oluşturur.

Strengths (Güçlü Yönleri)	Weaknesses (Zayıf Yönler)
• Açık standart yapısı ve geniş topluluk desteği • TLS/Secure WebSocket güvenliği (OCPP 2.0.1) • Merkezi yönetim ve log takibi • Güncellenebilir protokol mimaris	• Eski sürümlerde kimlik doğrulama eksikliği • Oturum yönetiminde standardizasyon eksikliği • Donanım güncellemelerinde gecikme • Ağ izleme yetersizliği
Opportunities (Fırsatlar)	**Threats (Tehditler)**
• Makine öğrenimi tabanlı anomali tespiti • OAuth 2.0 / JWT entegrasyonu • Güvenli yazılım yaşam döngüsü • Sertifikasyon ve yasal düzenlemeler	• Kimlik hırsızlığı ve yetkisiz erişim • MITM saldırıları • Veri manipülasyonu / faturalandırma sahtekarlığı • APT ve zincirleme tehditler

Sonuç ve Öneriler

- **Kısa Vadeli Çözüm:**
  TLS 1.3 zorunluluğu, güvenli token yönetimi ve oturum sonlandırma politikalarının uygulanması.
- **Orta Vadeli Çözüm:**
  OCPP 2.0.1 sürümüne geçiş, merkezi izleme sistemlerinin (SIEM) devreye alınması.
- **Uzun Vadeli Çözüm:**
  AI tabanlı saldırı tespiti sistemleri ve otomatik güvenlik denetimleriyle sürekli izleme.

Hazırlayan: Doğuş Bışaroğlu