SWOT Analizi

Strengths (Güçlü Yönler)

- **OCPP'nin yaygın kullanımı**: Şarj istasyonları ile merkezi sistemler arasında standartlaşmış bir iletişim protokolü mevcut.
- **OCPP 2.0.1 ile gelişmiş güvenlik desteği**: Yeni sürümlerde kimlik doğrulama, TLS ve komut yetkilendirme gibi mekanizmalar yer alıyor.
- **Modüler mimari**: Güvenlik özellikleri sonradan eklenebilir, backend ve şarj istasyonu yazılımlarına uygulanabilir.
- **Endüstri referansları ve uluslararası standartlar**: ISO 15118, IEC 61851, OWASP gibi rehberlik sağlayan güçlü ekosistem bulunuyor.

Weaknesses (Zayıf Yönler)

- **OCPP 1.6 ve önceki sürümlerde kimlik doğrulama eksikliği**: Yetkisiz komutlara açık.
- **Güvenli kanal (TLS) kullanımının isteğe bağlı olması**: Birçok üretici TLS'i varsayılan olarak pasif bırakıyor.
- **Backend tarafında komut yetkilendirme kontrolü eksik olabiliyor**: "Bu komutu gönderen gerçekten yetkili mi?" kontrolü çoğu sistemde tanımlı değil.
- **Audit log ve SIEM entegrasyonlarının eksikliği**: Saldırılar fark edilmeyebiliyor.
- **Konfigürasyon değişikliklerinin cihaz davranışını doğrudan etkilemesi**: Küçük bir yetkisiz komut büyük işletme problemlerine yol açabiliyor.

Opportunities (Fırsatlar)

- **Güvenli şarj altyapısına artan ihtiyaç**: EV pazarının büyümesiyle güvenlik yatırımları zorunlu hale geliyor.
- **Mutual TLS, sertifika yönetimi ve Zero Trust yaklaşımlarına geçiş fırsatı**.
- **OCPP 2.0.1 geçiş projeleri**: Güvenlik açıklarının kapatılması için sistemlerin güncellenmesi planlanabilir.
- **Regülasyonların sıkılaşması**: Güvenlik gereksinimlerinin yasal zorunluluk haline gelmesi pazarı güçlendirebilir.
- **Güvenlik testleri ve SIEM entegrasyonu için yeni ürün/hizmet fırsatları**.

Threats (Tehditler)

- **Yetkisiz RemoteStop, Reset, ChangeConfiguration saldırıları**: Hizmet kesintisi, müşteri kaybı ve marka itibarının zarar görmesi.
- **Man-in-the-Middle saldırıları**: TLS olmayan ortamlarda mesaj manipülasyonu.

- **Büyük ölçekli şarj ağlarına yönelik zincirleme saldırılar**: On binlerce istasyon etkilenebilir.
- **Fiziksel hasar veya aşırı yükleme riskleri**: Yanlış konfigurasyonlarla donanım zarar görebilir.
- **Siber saldırganların EV altyapısını hedef olarak seçmesi**: Enerji sektörünün kritik altyapı olması nedeniyle saldırı yüzeyinin artması.