SWOT Analizi: OCPP 1.6 Fiyatlandırma ve Erişim Kontrolü Manipülasyonu (MitM Saldırısı)

1. GÜÇLÜ YÖNLER (Strengths)

(Saldırgan açısından bu zafiyetin avantajları)

- **Geniş Saldırı Yüzeyi:** Saldırı, "en yaygın kullanılan protokol olan OCPP 1.6"yı hedef almaktadır.
- **Bilinen Zafiyetler:** Saldırı, TLS 1.2 kullanılmasına rağmen mevcut olan "zayıf şifre paketlerine" veya "sertifika doğrulamasının düzgün yapılandırılmamasına" dayanır.
- **Erişilebilir Vektörler:** Araya girmek için "ARP Spoofing veya sahte Wi-Fi erişim noktası" gibi yaygın ve erişilebilir yöntemler kullanılabilir.

2. ZAYIF YÖNLER (Weaknesses)

(Saldırgan açısından bu saldırının zorlukları veya kısıtlamaları)

- **Ağ Konumlanması Zorunluluğu:** Saldırganın, kendisini Şarj İstasyonu (CS) ile Merkezi Yönetim Sistemi (CSMS) arasına fiziksel veya mantıksal olarak konumlandırması (örn. yerel ağa sızması) gerekmektedir.
- **Şifre Kırma Gereksinimi:** Saldırı, zayıf yapılandırılmış olsa bile, mevcut "şifreli iletişimi (TLS) kırmayı" gerektirir.
- **Protokol Sınırlaması:** Bu senaryo, spesifik olarak "OCPP 1.6 (WebSocket)" protokolünün zayıf uygulamaları ile sınırlıdır.

3. FIRSATLAR (Opportunities)

(Saldırganın bu saldırıdan elde edeceği kazançlar)

- **Doğrudan Finansal Kazanç:** "Şarj ücretini kendi lehine manipüle ederek" fatura sahtekârlığı yapabilme.
- **Enerji Hırsızlığı:** Yetkisi olmayan bir kimlik kartına (idTag) erişim izni vererek "enerji hırsızlığı yapabilme".
- **Kritik Veri Hırsızlığı:** Sistemin "şarj ücretlendirme tarifesi bilgisini" (prices) ve "erişim kontrol politikalarını" (access control policies) sızdırabilme.
- **Sistem Manipülasyonu:** "Erişim kontrol politikalarını manipüle ederek" sistemin kimlik doğrulama mantığını değiştirebilme.

4. TEHDİTLER (Threats)

(Bu zafiyetin ekosistem için oluşturduğu genel tehditler)

- **Çoklu Güvenlik İhlali:** Zafiyet, sistemin aynı anda "Ortadaki Adam Saldırısı", "Zayıf Şifreleme" ve "Yetkisiz Erişim" gibi temel güvenlik prensiplerini ihlal etmesine neden olur.
- **Finansal ve Operasyonel Kayıp:** Fatura sahtekârlığı ve enerji hırsızlığı, şarj ağı operatörü için ciddi finansal ve operasyonel kayıplara yol açar.
- **Sistem Otoritesinin Kaybı:** Erişim kontrol politikalarının manipüle edilebilmesi, merkezi sistemin (CSMS) ağ üzerindeki otoritesini ve güvenilirliğini kaybetmesi tehdidini doğurur.