DOKÜMAN İÇERİĞİ BAŞLANGICI

**Anomali Senaryosu Adı:** OCPP 1.6 Fiyatlandırma ve Erişim Kontrolü Manipülasyonu (MitM Saldırısı)

**Sorumlu Kişi:** Furkan Akkamış

**Senaryo Açıklaması:** Bu anomali senaryosu, en yaygın kullanılan protokol olan OCPP 1.6 (WebSocket) üzerinde bir "Ortadaki Adam" (Man-in-the-Middle - MitM) saldırısının gerçekleştirilmesini kapsar.

**Zafiyet:** OCPP 1.6'nın TLS 1.2 şifrelemesi kullanmasına rağmen, zayıf şifre paketlerine (weak cipher suites) izin vermesi veya sertifika doğrulamasının düzgün yapılandırılmaması, saldırganın iletişimi deşifre edip araya girmesine olanak tanır.

**Saldırı Adımları:**

1. **Araya Girme:** Saldırgan, kendisini Şarj İstasyonu (CS) ile Merkezi Yönetim Sistemi (CSMS) arasına konumlandırır (Örn: ARP Spoofing veya sahte Wi-Fi erişim noktası ile).
2. **Veri Sızdırma:** Şifreli iletişimi (TLS) kırarak, CS ve CSMS arasında gidip gelen OCPP mesajlarını okumaya başlar.
3. **Hedefli Manipülasyon:** Kaynak makalede belirtildiği gibi (Garofalaki, 2022), saldırgan özellikle şu kritik bilgileri hedef alır:
    - **prices (Fiyatlar):** Şarj ücretlendirme tarifesi bilgisini sızdırabilir veya değiştirebilir.
    - **access control policies (Erişim Kontrol Politikaları):** Hangi idTag (kimlik kartı) yetkisine sahip olduğunu belirleyen politikaları sızdırabilir veya manipüle edebilir.
4. **Saldırı Çıktısı:** Saldırgan, ya şarj ücretini kendi lehine manipüle edebilir (fatura sahtekârlığı) ya da yetkisi olmayan bir kimlik kartına (idTag) erişim izni vererek enerji hırsızlığı yapabilir.

Bu senaryo, hocamızın derste belirttiği "Ortadaki Adam Saldırısı", "Zayıf Şifreleme" ve "Yetkisiz Erişim" başlıklarını doğrudan adreslemektedir.

**Kaynak Makale (Dayanak):** Garofalaki, Z., et al. (2022). "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)". *IEEE Communications Surveys & Tutorials*, 24(3), 1836-1875. DOI: 10.1109/COMST.2022.3184448