Başlık: EV Şarj Güvenliğinde Kritik Zafiyet Analizi: Duplicate Booking Simülasyonu

Elektrikli araç şarj altyapılarında (CSMS ve CP) güvenlik, sadece ağ şifrelemesi ile sınırlı değildir. Protokollerin oturum yönetimi mantığındaki açıklar, ciddi manipülasyonlara ve hizmet hırsızlığına kapı aralayabilir.

Şirket içi güvenlik laboratuvarımızda bugün gerçekleştirdiğimiz simülasyonda, literatürde **"A4: Duplicate Booking"** olarak bilinen saldırı vektörünü ve etkilerini başarıyla analiz ettik.

🛠️ **Teknik Analiz ve Simülasyon Adımları:** OCPP protokolünün bazı uygulamalarında görülen "Zayıf Oturum Yönetimi" (Weak Session Management) zafiyetine odaklandık. Simülasyonumuzda şu akışı doğruladık:

1. **Veri Keşfi:** Meşru bir `ReservationID` verisi ağ trafiği üzerinden tespit edildi.
2. **Phantom CP (Hayalet İstemci):** Saldırgan, ele geçirdiği bu ID ile kendini yetkili bir şarj noktası gibi göstererek CSMS'e `StartTransaction` talebi gönderdi.
3. **Zafiyetin Tetiklenmesi:** Merkezi Sistem (CSMS), rezervasyon kodunun geçerli olduğunu doğruladı; ancak bu kodun halihazırda aktif/çakışan bir oturumda olup olmadığını (Session Uniqueness) kontrol etmedi.
4. **Sonuç:** Sistem, sahte talebi onaylayarak yetkisiz enerji akışını başlattı.

📉 **Operasyonel ve Ekonomik Etkiler:** Bu zafiyet, saldırganların ücretsiz şarj hizmeti almasına (Hizmet Hırsızlığı), operatörler için gelir kaybına ve meşru kullanıcılar için Hizmet Reddine (DoS) neden olmaktadır. Ayrıca, mükerrer veri girişi nedeniyle CSMS raporlama bütünlüğü bozulmaktadır.

Bu testler, sadece zafiyetleri bulmak için değil; **Oturum Benzersizliği Kontrolü** ve **MFA tabanlı Boot Notification** gibi mitigasyon stratejilerini altyapılarınıza entegre etmek için kritik öneme sahiptir.

Şarj ağınızın bu tip mantıksal saldırılara karşı ne kadar dirençli olduğunu test ettiniz mi?

#InfoSec #EVCyberSecurity #ChargePoint #VulnerabilityAssessment #OCPPSecurity #SmartGrid #PenetrationTesting #ElectricVehicles

2. Görsel Tasarım Brifingi

Teknik bir gönderi olduğu için görselin "olayı anlatan" bir şema veya infografik olması en yüksek etkileşimi sağlayacaktır.

Önerilen Konsept: "İkiz Oturum (The Twin Session)" Şeması

Bu görsel, teknik detayı okumayan birinin bile sorunu saniyeler içinde anlamasını sağlar.

- **Arka Plan:** Koyu lacivert veya antrasit (Kurumsal/Tech hissi).
- **Merkez:** Bir Sunucu ikonu (CSMS'i temsil eder).
- **Sol Taraf (Meşru):**

    - Bir Elektrikli Araç ve Şarj İstasyonu ikonu.
    - Sunucuya giden bir ok (Yeşil Renk).
    - Ok üzerinde metin: `Reservation ID: #USER_01`
- **Sağ Taraf (Saldırgan):**
    - Bir Laptop veya "Hacker" silüeti (Phantom CP).
    - Sunucuya giden bir ok (Kırmızı Renk).
    - Ok üzerinde metin: `Reservation ID: #USER_01` (Sol taraftakiyle birebir aynı ID).
- **Çarpışma Noktası:** Sunucunun üzerinde veya yanında bir ünlem işareti ⚠️
- **Vurgu Metni:** Görselin altına veya üstüne büyük puntolarla: *"Weak Session Management: Duplicate Booking Detected"*

Alternatif Konsept: Kod/Terminal Görünümü

Daha "hacker" vari bir hava katmak isterseniz:

- Siyah bir terminal ekranı görüntüsü.
- Yeşil kod satırları arasında bir hata mesajı:
    - `> StartTransaction(Rid: 5542) ... APPROVED`
    - `> StartTransaction(Rid: 5542) ... APPROVED (WARNING: DUPLICATE SESSION)`
- Arka planda şirket logosu flu şekilde.

3. Paylaşım İpuçları

1. **Etiketleme (Mentions):** Eğer bu çalışmayı bir iş ortağıyla veya belirli bir donanım üzerinde yaptıysanız onları etiketleyin. Ayrıca EV güvenliğiyle ilgilenen global organizasyonları (örn. Open Charge Alliance) etiketlemek görünürlüğü artırabilir.
2. **İlk Yorum (Call to Action):** Gönderiyi paylaştıktan hemen sonra ilk yoruma web sitenizin iletişim linkini veya varsa konuyla ilgili blog yazınızı ekleyin.
    - *Örnek:* "Bu zafiyetin detaylı teknik analizi ve çözüm önerilerimiz için blog yazımızı inceleyebilirsiniz: [Link]"
3. **PDF Eklentisi:** Eğer hazırladığınız raporun (bu konuşmanın başındaki teknik raporun) özet bir versiyonu (1-2 sayfa) varsa, LinkedIn'in "Document" özelliği ile gönderiye PDF olarak eklemek, sadece resim paylaşmaktan %300 daha fazla erişim sağlar.