OCPP (Yetki Yükseltme) - Yerel Liste Manipülasyonu (Privilege Escalation)

1. Anomali Tanımı

Saldırganın istasyonun Local Authorization List (Yerel Yetki Listesi) içine kendi ID'sini (ör. RFID, Mobile ID) ekleyerek yetkisiz erişim/şarj başlatması. Bu, yetki seviyesinin yükseltilmesi (privilege escalation) olarak sınıflandırılır ve özellikle çevrimdışı modlarda istasyonların yerel listelere güvendiği senaryolarda etkilidir.

2. Gözlemler / Tespit Edilecek Belirtiler

• Yetki listesinde beklenmeyen değişiklikler (sürüm numarası, imza eksikliği).

• Oturum açma kayıtlarında tanımlanamayan veya aynı ID ile çakışan oturumlar.

• Anormal artışta başarısız/başarılı kimlik doğrulama sayıları.

3. Tespit Yöntemleri / Teknikler

• Bütünlük kontrolü: Local Authorization List dosyalarının hash/checksum analizi ve karşılaştırması.

• Signed updates: Yetki listesi güncellemelerinin dijital imzasının doğrulanması.

• Merkezi ile kıyaslama: Lokal liste ile CPMS'deki merkezi liste periyodik olarak çapraz kontrol edilecek.

4. Olası Sebepler / Zafiyetler

• Listelerin imzasız veya zayıf anahtar yönetimi ile güncellenmesi.

• Çevrimdışı çalışmaya bırakılmış istasyonlarda aşırı yetki verme (OfflineTxForUnknownIdEnabled gibi ayarların yanlış konfigürasyonu).

5. Etki / Riskler

• Yetkisiz ücretsiz şarj kullanımı ve gelir kaybı.

• Hatalı faturalama, müşteri güveni erozyonu.

• Çoklu istasyonlarda tekrarlanırsa operasyonel ve yasal sorunlar.

6. Önerilen Önlemler / Mitigasyonlar

• Tüm yetki listesi güncellemelerinin dijital olarak imzalanması ve imza doğrulaması.

• Çevrimdışı kimlik doğrulamaya bağımlılığı azaltma; kritik kararlar için merkezi doğrulama veya zaman sınırlı offline listeler kullanma.

• D01 Use Case: Yetki listesi güncelleme süreçleri için audit / rollback mekanizmaları kurulması.

• Log ve değişiklik izleme: Yetki liste değişiklikleri için IMMEDIATE alarm ve forensik kayıt tutulması.

7. İlgili Referanslar

(Alcaraz, et al., 2023). OCPP use cases on Local Authorization List and C13 UC. [cite refs: 504, 511, 759, 774]