Kapsamlı Saldırı Senaryosu: "Operasyonel Felç" (Yaygın Hizmet Reddi - DoS)

Bu belge, "Anormal Protokol Etkileşimleri" dokümanındaki prensiplere (özellikle Bölüm 2.1) dayanan "Yaygın Hizmet Reddi" senaryosunu detaylandırmak için hazırlanmıştır.

1. Senaryo Özeti

"Operasyonel Felç", bir saldırganın bir Şarj Noktası Operatörü'ne (CPO) ait çok sayıda şarj istasyonunu (EVSE) eş zamanlı olarak hedef alarak, meşru kullanıcıların hizmet almasını engellediği, kasti bir Hizmet Reddi (Denial of Service - DoS) saldırısıdır. Saldırı, OCPP protokolünün operasyonel komutlarını (örn. `RemoteStopTransaction`) kötüye kullanarak, aktif şarjları toplu halde durdurmayı veya CSMS'i sahte mesajlarla boğarak tüm ağı kilitletmeyi amaçlar. Sonuç, anlık bir operasyonel kaos, gelir kaybı ve ciddi bir itibar zedelenmesidir.

2. Senaryonun Amacı

- **Birincil Amaç:** Bir CPO'nun tüm şarj ağını veya belirli bir bölgedeki istasyonlarını toplu olarak devre dışı bırakmak, sistemi meşru kullanıcılar için erişilemez hale getirmek ve operasyonel kaosa yol açmak.
- **İkincil Amaç:** Aktif şarj işlemlerini zorla ve aniden sonlandırarak kullanıcı memnuniyetini sabote etmek, CPO'ya doğrudan anlık gelir kaybı yaşatmak ve marka itibarına kalıcı hasar vermek.

3. Hedef Varlıklar ve Temel Zafiyetler

- **Hedef Varlık:** EVSE ağı, Merkezi Yönetim Sistemi (CSMS) ve aradaki OCPP iletişim kanalı.
- **Zafiyet 1 (Ağ Katmanı):** Zayıf Kimlik Doğrulama (OCPP Güvenlik Profili 1 veya 2). Karşılıklı sertifika (mTLS) kullanılmaması, saldırganın kendini meşru bir CSMS olarak tanıtmasına (Spoofing) olanak tanır. (PDF Ref: Bölüm 2.1)
- **Zafiyet 2 (Ağ Katmanı):** Güvensiz veya şifrelenmemiş ağ iletişimi. Saldırganın bir "Ortadaki Adam" (MitM) saldırısıyla araya girip komutları yakalamasına veya enjekte etmesine izin verir.
- **Zafiyet 3 (Uygulama Katmanı):** CSMS tarafında Hız Sınırlaması (Rate Limiting) veya davranışsal analiz eksikliği. Bu durum, bir saldırganın kısa sürede binlerce anormal komut göndermesine karşı sistemi savunmasız bırakır.

4. Saldırı Yöntemleri ve Adım Adım Yürütme

Saldırı, iki ana vektör üzerinden gerçekleştirilebilir:

Vektör A: Toplu Oturum Sonlandırma (Aktif Kullanıcılara Yönelik)

1. **Hazırlık ve Erişim:** Saldırgan, bir grup istasyonun ağ trafiğini (MitM - Zafiyet 2) izleyebileceği bir konuma gelir veya zayıf kimlik doğrulamayı (Zafiyet 1) kullanarak sahte bir CSMS gibi davranır.

2. **Keşif:** Saldırgan, ağdaki `StatusNotification` (Durum Bildirimi) mesajlarını izleyerek veya tahmin yürüterek 'Charging' (Şarj Oluyor) durumundaki istasyonları tespit eder.
3. **Toplu Saldırı:** Saldırgan, hedef aldığı tüm aktif istasyonlara *eş zamanlı olarak* veya çok hızlı bir döngü içinde `RemoteStopTransaction` (Uzaktan İşlemi Durdur) komutları gönderir.
4. **Fiziksel Sonuç:** Ülkenin/bölgenin farklı yerlerindeki yüzlerce (veya binlerce) elektrikli aracın şarjı aniden kesilir. İstasyonlardaki röleler açılır ve oturumlar sonlanır. Kullanıcılar, araçlarının başında ne olduğunu anlayamaz ve CPO'nun müşteri hizmetleri kilitlenir.

Vektör B: CSMS Sel Baskını (Sistemi Kilitleme)

1. **Hazırlık:** Saldırgan, ele geçirdiği birkaç EVSE'yi (veya bir botnet ağını) veya yine sahte bir CSMS kimliğini (Zafiyet 1) kullanır.
2. **Sistemik Saldırı:** Saldırgan, hedef CPO'nun CSMS sunucusuna yönelik binlerce sahte mesaj gönderir.
3. **Sahte Önyükleme (BootNotification Flood):** Saldırgan, CSMS'e saniyede binlerce sahte `BootNotification` (Önyükleme Bildirimi) mesajı yağdırır. (PDF Ref: Bölüm 2.1). CSMS, bu sahte "merhaba, ben yeni açıldım" mesajlarını işlemekten kaynakları (CPU, RAM, veritabanı bağlantıları) tükenir ve kilitlenir.
4. **Siber Sonuç:** CSMS kilitlendiği için, meşru istasyonlardan gelen `MeterValues` (Sayaç Değerleri) gibi kritik verileri işleyemez, yeni şarj taleplerini (`Authorize`) onaylayamaz. Tüm ağ fiilen durmuş olur.

5. İlgili Tehditler (STRIDE Modeli)

- **D - Denial of Service (Hizmet Reddi):** Saldırının ana kategorisi ve amacıdır. Sistemin meşru işlevini yerine getirmesi engellenir.
- **S - Spoofing (Kimlik Sahtekarlığı):** Saldırganın, Vektör A veya B'yi gerçekleştirebilmek için meşru bir CSMS sunucusunu veya meşru bir EVSE'yi taklit etmesi gerekebilir.

6. Anomali Göstergeleri ve Tespit Yöntemleri

- **Ana Gösterge:** CSMS loglarında, normal operasyonel kalıpların dışında, anormal derecede yüksek sayıda ve sıklıkta `RemoteStopTransaction` komutunun gözlemlenmesi.
- **Korelasyon Eksikliği:** Çok sayıda şarj oturumunun, kullanıcı talebi (`StopTransaction`), tam şarj (`EVFull`) veya şebeke kesintisi gibi meşru bir neden olmaksızın, *aynı anda* sonlanması.
- **Ağ Davranışı:** Tek bir IP adresinden veya IP bloğundan, normal bir istasyonun gönderebileceğinden çok daha fazla `BootNotification` veya `Heartbeat` (Kalp Atışı) mesajı gelmesi.
- **Operasyonel Geri Bildirim:** Müşteri hizmetlerine, farklı lokasyonlardan "şarjım aniden durdu" veya "istasyon çalışmıyor" şikayetlerinin aniden yığılması.

7. Önlemler ve Azaltma Stratejileri

1. **Ağ Güvenliğini Sağlama (Zafiyet 1 ve 2'ye karşı):**

    - **Zorunlu OCPP Güvenlik Profili 3 Kullanımı:** Karşılıklı TLS (mTLS) sertifika doğrulamasını zorunlu kılmak. Bu, sahte CSMS (Spoofing) saldırılarını ve MitM komut enjeksiyonunu büyük ölçüde engeller. (PDF Ref: Bölüm 4.1)
2. **Uygulama Güvenliğini Artırma (Zafiyet 3'e karşı):**
    - **Akıllı Hız Sınırlaması (Rate Limiting):** CSMS tarafında, kritik komutlar (`RemoteStopTransaction`, `BootNotification` vb.) için istasyon başına veya IP başına akıllı hız sınırları uygulamak. (Örn: Bir istasyon 1 dakika içinde 3'ten fazla `BootNotification` gönderemez).
    - **Davranışsal Analiz:** Bir anomali tespit sisteminin (IDS) "Normal operasyonda bir CPO, 1 saniye içinde 500 farklı istasyona 'durdur' komutu göndermez" kuralını bilmesi ve bu tür anormal toplu komutları bloke etmesi veya bir operatör onayına sunması.
3. **Dayanıklılık ve Hızlı Müdahale:**
    - **CSMS Yedekliliği:** DoS saldırılarına karşı yük dengeleyiciler (load balancers) ve coğrafi olarak yedekli CSMS sunucuları kullanmak.
    - **Acil Durum Prosedürü:** Toplu bir DoS saldırısı tespit edildiğinde, etkilenen istasyonların güvenli iletişim kanallarını (örn. VPN tünelleri) otomatik olarak sıfırlayıp yeniden kuracak veya şüpheli komutları geçici olarak yoksayacak bir "kilitlenme" (lockdown) modu tanımlamak.