RAPOR: SİMÜLASYON ORTAMI GEREKSİNİMLERİ

Senaryo Adı: Sahte Firmware Güncellemesi ile Şarj İstasyonunu Ele Geçirme (Ransomware)

Bu simülasyon, bir saldırganın **OCPP v2.0.1** protokolündeki **güvensiz firmware güncelleme (L02)** kullanım durumunu istismar ederek bir Şarj İstasyonu'nu (CS) ele geçirmesini modellemek üzere tasarlanmıştır.

1. Temel Ağ Topolojisi ve Bileşenler

Simülasyon, izole edilmiş bir sanal ağ üzerinde çalışan üç ana sanal makineyi veya konteyneri gerektirir:

Bileşen Adı	Rolü ve Amacı	Gerekli Yazılımlar / Özellikler
Charge Point (CS)	**Birincil Hedef Varlık.** Zafiyetli konfigürasyona sahip Şarj İstasyonu yazılımını barındırır.	**OCPP v2.0.1 Uygulaması:** İstemci rolünde, güvensiz L02 kullanımını destekleyecek (kaynak/imza doğrulaması yapmayacak) şekilde konfigüre edilmeli. **İşletim Sistemi:** Firmware yüklemesi sonrası fidye yazılımı (PoC) betiği çalıştırabilecek bir Linux dağıtımı (örn: Debian/Ubuntu).
Charge Point Management System (CSMS)	**Meşru Yönetim Sistemi.** CS ile rutin iletişimi sağlar ve saldırganın kimliğine bürüneceği hedefi temsil eder.	**OCPP v2.0.1 Sunucusu:** CS ile bağlantı kurabilen ve `UpdateFirmware` komutunu gönderebilen bir açık kaynaklı CSMS simülatörü (örn: SteVe veya benzeri bir araç).

Attacker Machine (ATK)	**Saldırgan İş İstasyonu.** MitM saldırısını ve sahte CSMS rolünü üstlenir.	**MitM Aracı:** Ağ trafiğini dinlemek ve yönlendirmek için Bettercap, mitmproxy veya Scapy. **OCPP İstemcisi/Sunucusu:** Doğrudan sahte UpdateFirmware komutu gönderebilen veya MitM üzerinden meşru komutu değiştirebilen özel betik. **Web Sunucusu:** Sahte Ransomware **Payload**'unu (firmware dosyası) barındırmak için hafif bir HTTP sunucusu.

2. Kritik Konfigürasyon Değişiklikleri (Zafiyet Enjeksiyonu)

Senaryonun başarılı şekilde simüle edilebilmesi için, aşağıdaki zafiyetlerin hedef sistemlere (CS) kasıtlı olarak enjekte edilmesi/konfigüre edilmesi şarttır:

A. Güvenlik Profilinin Düşürülmesi (Ağ Zafiyeti)

- **Hedef:** CS ve CSMS arasındaki iletişim kanalı.
- **Değişiklik:** İletişimin ya şifresiz **WebSocket (WS)** üzerinden yapılması ya da **karşılıklı sertifika doğrulamasının (mTLS)** (Profil 3 gerekliliği) devre dışı bırakılması.
- **Amaç:** Saldırganın (ATK) araya girip (MitM) trafiği dinlemesi ve değiştirmesi kolaylaşır.

B. Firmware Doğrulama Eksikliği (Protokol Zafiyeti)

- **Hedef:** CS üzerindeki firmware yükleme bileşeni.
- **Değişiklik:** CS'in, gelen `UpdateFirmware` isteğinde belirtilen dosyayı indirip kurarken, **ne CSMS sertifikasının kaynağını ne de firmware paketinin dijital imzasını/bütünlüğünü kontrol etmemesi** (yani, L02 kullanım durumunun aktif ve güvensiz olması).
- **Amaç:** Saldırganın hazırladığı kötü amaçlı firmware (ransomware PoC) paketi, sistem tarafından meşru bir güncelleme olarak algılanır ve kurulur.

3. Ransomware Simülasyonu (Payload)

- **Bileşen:** Sahte Firmware Paketi (Ransomware Payload).
- **İçerik:** Gerçek bir fidye yazılımı yerine, simülasyon amaçlı olarak, yükleme sonrası çalışacak ve şunları yapacak bir **Proof-of-Concept (PoC) betiği** kullanılmalıdır:

1. CS'in ana şarj hizmetlerini (OCPP bağlantısı, şarj soketi kontrolü vb.) durdurmak veya kilitlemek.
2. Fiziksel ekranı (simülasyonda konsol çıktısı veya bir web arayüzü) **"Sistem Kilitlendi. Fidye Talep Ediliyor"** gibi bir mesajla değiştirmek.
3. CSMS'e bir hata mesajı göndermek veya tamamen çevrimdışı kalmak.

4. Simülasyon Senaryosu Adımları (Teknik Uygulama Özeti)

1. **Ağ Kurulumu:** Üç bileşen (CS, CSMS, ATK) tek bir izole sanal ağa bağlanır.
2. **MitM Başlatma:** ATK makinesi, CS ile CSMS arasındaki trafiği kendi üzerinden yönlendirmek için ARP zehirlenmesi başlatır.
3. **Saldırı Başlatma:** ATK, ya MitM üzerinden meşru bir güncelleme komutundaki URL'yi kendi sunucusuna yönlendirir ya da doğrudan CSMS kimliğine bürünerek sahte `UpdateFirmware` isteği gönderir.
4. **Ele Geçirme:** CS, güvensiz L02 konfigürasyonu nedeniyle sahte firmware'i indirip kurar ve yeniden başlar. Yeniden başlatma sonrası Ransomware PoC betiği çalışır ve istasyon hizmet dışı kalır (DoS).