RAPOR: ANOMALİ SENARYOSU 1

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

1. Senaryo Özeti

Bu senaryo, bir elektrikli araç şarj istasyonunun (CS) firmware güncelleme mekanizmasındaki bir zafiyetin istismar edilmesini detaylandırmaktadır. Saldırgan, Merkezi Şarj İstasyonu Yönetim Sistemi (CSMS) gibi davranarak şarj istasyonuna kötü amaçlı bir yazılım (özellikle fidye yazılımı — ransomware) yükler. Başarılı saldırı sonucunda şarj istasyonu kilitlenir, hizmet veremez hale gelir ve istasyon ekranında fidye talebi görüntülenir.

2. Hedef Varlıklar

- **Birincil Hedef:** Halka açık, denetimsiz alanlara yerleştirilmiş Şarj İstasyonları (CS).
- **İkincil Hedefler:** Şarj hizmeti alan son kullanıcılar ve istasyon operatörünün (CSO) itibarı.

3. İlgili Zafiyetler

Senaryonun temel dayanağı, OCPP v2.0.1 protokolü ve uygulamalarındaki spesifik zafiyetlerdir:

1. **Güvensiz Güncelleme Seçeneği:** Protokolün hâlâ "Güvensiz Firmware Güncelleme" (L02 kullanım durumu) seçeneğini barındırması.
2. **Doğrulama Eksikliği:** L02 kullanım durumunda olduğu gibi, firmware'in kaynağını (CSMS sertifikası) veya firmware paketinin bütünlüğünü (dijital imza) doğrulamayan veya zayıf doğrulayan sistemlerin hedef alınması.
3. **Ağ Zafiyetleri:** CS ile CSMS arasındaki iletişimin, Ortadaki Adam (Man-in-the-Middle / MitM) saldırılarına karşı yeterince korunmasız olması (örneğin, düşük güvenlik profili kullanılması).

4. Tehdit Kategorisi

Bu saldırı STRIDE modelindeki birden fazla kategoriyi kapsamaktadır:

- **Spoofing (Kimlik Hırsızlığı):** Saldırganın kendisini meşru bir CSMS olarak tanıtması.
- **Tampering (Kurcalama):** Meşru firmware paketinin, kötü amaçlı olanla değiştirilmesi.
- **Repudiation (İnkâr):** Saldırının kaynağının gizlenmesi (saldırı CSMS'ten geliyormuş gibi görünür).

- **Information Disclosure (Bilgi İfşası):** İstasyonun firmware sürümü veya ağ yapılandırması gibi bilgilerin önceden sızdırılmış olması.
- **Denial of Service (Hizmet Reddi):** İstasyonun kilitlenerek hizmet veremez hale gelmesi.
- **Elevation of Privilege (Yetki Yükseltme):** Saldırganın, firmware yükleyerek istasyon üzerinde en yüksek sistem ayrıcalıklarını elde etmesi.

5. Saldırı Vektörü ve Adımları

1. **Keşif:** Saldırgan, L02 kullanım durumu aracılığıyla güvensiz firmware güncellemelerine izin veren bir şarj istasyonu ağını belirler.
2. **Hazırlık:** İstasyonun işletim sistemine uyumlu, cihazı kilitleyen ve ekranda fidye notu gösteren özel bir firmware (ransomware) paketi hazırlanır.
3. **Enjeksiyon (Saldırı):** Saldırgan, CSMS ile CS arasındaki ağa sızarak (MitM saldırısı) meşru bir güncelleme işlemi sırasında, CSMS'ten geliyormuş gibi sahte ve kötü amaçlı firmware paketini şarj istasyonuna gönderir.
4. **Yürütme:** CS, gelen paketi güvensiz L02 protokolü uyarınca doğrulamadan veya zayıf bir doğrulamayla kurar ve cihazı yeniden başlatır.
5. **Ele Geçirme:** Yeniden başlatma sonrası, fidye yazılımı devreye girer. İstasyonun tüm şarj fonksiyonları kilitlenir ve ekranda "Hizmetin açılması için fidye ödenmelidir" içerikli bir mesaj belirir.

6. Tespit Yöntemleri

- **Merkezi Sistem (CSMS):** Hedef CS'nin aniden çevrimdışı (offline) duruma geçmesi ve CSMS'ten gelen komutlara yanıt vermemesi.
- **Fiziksel Tespit:** Kullanıcıların veya teknik personelin, istasyon ekranındaki anormal fidye mesajını görmesi ve raporlaması.
- **Ağ İzleme:** Ağ trafiğinde, CSMS dışındaki şüpheli bir kaynaktan CS'ye doğru beklenmedik boyutta bir veri (firmware dosyası) aktarımının tespit edilmesi.

7. Potansiyel Etki ve Sonuçlar

- **Hizmet Reddi (DoS):** Şarj istasyonunun kullanılamaz hale gelmesi (Tehdit Sonucu TC-3).
- **Ekonomik Hasar:** Hem talep edilen fidye hem de hizmet kesintisinden kaynaklanan gelir kaybı (Etki Kodu I-3).
- **İtibar Kaybı:** Operatör firmanın (CSO) güvenilirliğinin ve marka imajının sarsılması.

8. İlgili Karşı Önlemler

1. **Güvenli Güncelleme Protokolü:** Güvensiz L02 kullanımı terk edilmeli; firmware güncellemeleri daima CSMS sertifikasının kaynağını ve firmware imzasını doğrulayan güvenli prosedürler (ör. L01) üzerinden yapılmalıdır.
2. **Güvenli İletişim Kanalı:** CS ve CSMS arasındaki iletişim, MitM saldırılarını önlemek için daima en yüksek güvenlik profili (Profil 3: TLS v1.3 ve karşılıklı sertifika doğrulama) ile şifrelenmelidir.
3. **Bütünlük Kontrolü:** İstasyonlar, yazılım bileşenlerinin bütünlüğünü periyodik olarak doğrulamak için hash fonksiyonları gibi kriptografik yöntemler kullanmalıdır.

Notlar:

- L02: OCPP spesifikasyonunda tanımlı "Güvensiz Firmware Güncelleme" kullanım durumu.
- TC-3 ve I-3 gibi kodlamalar örnek etki/sonuç sınıflandırmalarıdır; kurumunuzun risk matrisiyle eşleştirilmeleri önerilir.

9. Kaynaklar

https://irep.ntu.ac.uk/id/eprint/54419/1/2478037_Brown.pdf
https://www.usenix.org/system/files/vehiclesec25-boussaha.pdf
https://irep.ntu.ac.uk/id/eprint/54086/
https://www.osti.gov/servlets/purl/2431391