Kötü Amaçlı Bellenim Yüklemesi Yoluyla Araç İçi Ağa Yönelik Kalıcı Hizmet Reddi (P-DoS)

1. Amaç

Saldırganın temel amacı, şarj istasyonunun (CP / EVSE) zayıf bellenim (firmware) güncelleme mekanizmasını kullanarak cihazın ana kontrolcüsüne (MCU) kalıcı ve kötü amaçlı bir yazılım yerleştirmektir. Bu yazılımın nihai hedefi, şarj istasyonuna bağlanan herhangi bir aracın dahili CAN bus ağına en yüksek öncelikli (`0x00`) anlamsal veri paketleri göndererek aracın tüm kritik Elektronik Kontrol Üniteleri (ECU) arasındaki iletişimi kilitlemek ve aracı fiziksel olarak çalışamaz hale getirmektir.

2. Tehdit Kategorisi (STRIDE)

- **Kurcalama (Tampering):** Şarj istasyonunun belleniminin (firmware) yetkisiz bir sürümle değiştirilmesi.
- **Hizmet Reddi (Denial of Service - DoS):** Araç içi CAN bus ağının iletişim kapasitesinin %98'e varan oranda doyurulması ve kritik ECU'ların (Fren, Motor, ABS) iletişiminin engellenmesi.
- **Ayrıcalık Yükseltme (Elevation of Privilege):** İnternet (OCPP) üzerinden elde edilen sınırlı erişimin, aracın fiziksel kontrol ağı (CAN) üzerinde en yüksek ayrıcalıklı erişime dönüştürülmesi.

3. Ön Koşullar

1. **Ağ Konumu:** Saldırganın, hedef şarj istasyonunun ağ trafiğini izleyebileceği veya değiştirebileceği bir Ortadaki Adam (Man-in-the-Middle, MitM) konumu elde etmiş olması (örneğin, istasyonun bağlı olduğu yerel ağı veya güvensiz Wi-Fi'ı ele geçirerek).
2. **Zayıf CP Güvenliği:** Hedef CP'nin, bellenim güncellemelerinin kriptografik imzasını doğrulamayan güvensiz bir güncelleme sürecini (`L02 kullanım durumu`) desteklemesi.
3. **Protokol Bilgisi:** Saldırganın, CP'nin kullandığı `UpdateFirmware.req` OCPP komutunun yapısını ve CAN bus arbitrasyon mekanizmasının (düşük ID'nin yüksek önceliğe sahip olması) nasıl çalıştığını bilmesi.

4. Saldırı Vektörü ve Adım Adım Yürütme

Saldırı, birbirini takip eden iki ana aşamadan oluşur: (A) CP'nin ele geçirilmesi ve (B) Aracın devre dışı bırakılması.

Aşamalı Yürütme: A - CP'nin Ele Geçirilmesi (OCPP Saldırısı)

1. **Ağa Sızma ve Dinleme:** Saldırgan, MitM konumu üzerinden CP ve Merkezi Yönetim Sistemi (CSMS) arasındaki OCPP trafiğini pasif olarak dinler.
2. **Güncelleme Komutunun Yakalanması:** Saldırgan, CSMS tarafından gönderilen meşru bir `UpdateFirmware.req` komutunu yakalar. Bu komut, bellenimin indirileceği URL (konum) bilgisini içerir.

3. **Komutun Manipülasyonu (Tampering):** Saldırgan, yakaladığı bu komutu anlık olarak değiştirir. `location` (konum) parametresindeki meşru URL'yi, kendi kontrolündeki ve kötü amaçlı bellenimi barındıran sunucunun adresiyle değiştirir.
4. **Kötü Amaçlı Bellenimin Yüklenmesi:** CP, manipüle edilmiş komutu alır. Cihaz, güvensiz L02 sürecini kullandığı için bellenimin imzasını doğrulamaz. CP, saldırganın sunucusuna bağlanır, kötü amaçlı dosyayı indirir ve meşru bir güncelleme gibi kurar .
5. **Yerleşme ve Gizlenme:** Kötü amaçlı yazılım (rootkit), CP'nin ana denetleyicisine (MCU/SoC) yerleşir. Tespit edilmemek için normal OCPP işlevlerini (örn. `Heartbeat.req` göndermek) taklit etmeye devam eder ve bir sonraki adımdaki tetikleyiciyi bekler. Bu noktada şarj istasyonu artık bir "zombi" cihazdır.

Aşamalı Yürütme: B - Aracın Kilitlenmesi (CAN bus Saldırısı)

1. **Tetikleyicinin Algılanması:** Kötü amaçlı yazılım, aracın CP'ye fiziksel olarak bağlanmasını (örn. bir `StatusNotification` mesajının "Preparing" olarak tetiklenmesi veya CAN denetleyicisinden gelen bir sinyal) algılar.
2. **Protokol Köprüsünün Silahlandırılması:** Kötü amaçlı yazılım, CP'nin ana görevi olan "protokol köprüsünü" ele alır. Normalde bu köprü, OCPP komutlarını dahili CAN mesajlarına çevirirken, şimdi doğrudan aracın CAN bus hattına yazmak için kullanılır.
3. **CAN Paket Seli (Flooding) Başlatma:** Kötü amaçlı yazılım, aracın CAN bus ağına yönelik sürekli bir saldırı başlatır. Bu saldırı, CAN protokolünün temel bir zafiyetini sömürür:
    - Saldırgan, CAN ID'si `0x00` veya `0x01` (mümkün olan en yüksek öncelik) olan binlerce anlamsal veri paketi oluşturur.
    - Bu paketlerin veri yükünün (data payload) bir anlamı yoktur (örn. `00 00 00 00...`).
    - Bu paketler, CP'nin CAN alıcı-vericisi üzerinden saniyede yüzlerce kez (yüksek frekansta) araca enjekte edilir.
4. **Arbitrasyon (Tahkim) Kilitlemesi:** CAN bus protokolü, aynı anda gönderilen mesajlardan ID'si en düşük olanın (en öncelikli) hatta kalmasına izin verir (wired-AND).
5. Saldırganın `0x00` ID'li paketleri, diğer tüm meşru ECU'ların (Fren, ABS, Motor) paketlerinden (örn. ID `0x1A0`, `0x2B0` vb.) daha önceliklidir. Bu nedenle, meşru ECU'lar sürekli olarak "hattın boşalmasını" bekler, ancak hat hiçbir zaman boşalmaz.

5. Beklenen Fiziksel/Anormal Sonuç

- Aracın dahili iletişimi anında çöker.
- Aracın gösterge panelinde, "Motor Arızası", "ABS Arızası", "Fren Sistemi Hatası", "Hava Yastığı Arızası" gibi çok sayıda kritik hata ışığı aynı anda yanar ("Noel ağacı" etkisi).
- Araç "kontak" modundaysa, marş basmaz veya "drive-by-wire" sistemleri (elektronik gaz pedalı, fren) tepki vermez.
- Araç, şarj istasyonuna bağlı kaldığı sürece bu Kalıcı Hizmet Reddi (P-DoS) durumunda kalır. Bağlantı kesilse bile, ECU'larda oluşan kritik hata kodları (DTCs) nedeniyle aracın servise gitmeden çalışması mümkün olmayabilir.

6. Adli Bilişim İzleri (Forensic Artifacts)

1. **Araç Tarafında:** Aracın diyagnostik belleğinde (DTC logları), hemen hemen her ECU için "İletişim Kaybı" (U-serisi kodlar) ve "Bus Off" hata kayıtları bulunur.
2. **CSMS Tarafında:** `UpdateFirmware` komut günlüklerinde, şüpheli veya bilinmeyen bir IP/alan adına (attacker.com) ait bir URL kaydı.
3. **Şarj İstasyonu Tarafında:** Cihazdan alınan bellenim imajının (eğer mümkünse) hash değeri, üreticinin yayınladığı meşru bellenim hash değeriyle eşleşmez. CP'nin kendi ağ logları, CSMS'den gelmeyen, ancak CP'nin CAN denetleyicisi tarafından başlatılan anormal, yüksek frekanslı CAN paketlerini gösterir.