**Anomali Senaryoları Listesi**

1. **Uzaktan EVC kontrolü ile frekans/kararlılık saldırısı internete açık EV kontrol/baş yönetim sistemleri ele geçirilerek komutların/schedulingìn manipüle edilemesi ile yüzlerce istasyonun aynı anda başlatılıp durdurulmasıyla şebeke yükünde ani değişimleri yaratması.**
2. **DDoS/Rezarvasyon taahhütleriyle hizmet kesintisi Çok sayıda ele geçirilmiş EV veya sahte rezervasyon istekleriyle DDoS/rezervasyon taahhütleri üretilip halk istasyonlarının hizmet veremez hale getirilmesi**
3. **Enerji Akış parametrelerinin değiştirilmesi (MitM) OCPP veya iletişişm zaafiyetleri aracılığıyla şarj oranı / enerji akış parametrelerinin değiştirilmesi ile batarya hasarı veya şebeke aşırı yüklenmesi oluşturulması .**
4. **Sahte Yetki ile Ücretsiz Şarj OCPP oturumlarının veya kontrol merkezinin taklidini (impersonation) yoluyla istasyonları offline moda düşürülüp sahte yetki listesi ile kayıt dışı /ücretsiz şarj sağlanması.**
5. **SSFR ile İç Ağ Keşfi ve Bilgi Sızıntısı Server-Side Request Forgery (SSFR) veya benzeri teknikler ile EVCSMS üzerinden yerel ağdaki cihazlara istek yönlendirip iç dosyaların/logların okunması veya LAN keşfi yapılması**
6. **Rezervasyon/Kuyruk taşması sonucu veri/ işlem bozulması OCPP için önerilen bazı paylaşım/ kuyruk mekanizmalarının istasyon offline / kuyruklu çalıştığında tampon taşmasına ve kayıtsız şarj oturumları oluşturmasına yol açması.**
7. **Roamin pseudonym mekanizmasında lokasyon gizliliği ihlali Roaming-pseudonym mekanizmalarında TTP veya tedarikçi tarafından tutulan veriler ele geçirilirse kullanıcı konum ve kimlik bilgilerinin ilişkilendirilmesi mümkün olur.**
8. **Çalıntı Akıllı Kart / Cihaz Senaryosu ile ödeme suistimali Akıllı kart veya EV sahibi cihazın çalınması halinde çift-kimlik doğrulama olsa dahi yetkisiz şarj/ödeme suistimali yapılabilmesi.**
9. **Replay/Zamanlama saldırıları Protokol düzeyinde replay veya zamanlama sapması ile mesajların geciktirilip yeniden oynatılması sonucu yetkilendirme/işlem tekrarı veya bütünlük ihlali gerçekleştirilmesi**
10. **Anahtar türetme zaafiyeti (known-key/future-key ) Mevcut oturum anahtarlarından ileriki oturu anahtarlarının türetilebilmesi halinde geçmiş veya gelecek oturumların gizliliğinin bozulması riski.**
11. **Koordineli Yüksek Yük saldırıları Çok sayıda PEV/EVSEnin aynı anda yüksek güç çekmesiyle ani yük artışı yerel veya bölgesel aşırı yük / kararsızlık / black-out-riski.**
12. **Malware bulaşması ve yayılması Enfekte bir araç veya şark istasyonu , haberleşme kanallarıyla malware gönderip ağdaki diğer EVSE/PEV leri enfekte eder. Lateral hareketle geniş çaplı bozulma**
13. **OTA/Firmware güncelleme kötüye kullanılması Firmware güncelleme mekanizdmasının kötü sunucuya yönlendirilmesi veya imzasız güncelleme ile zararlı yazılım yüklenmesi.**
14. **Kimlik Doğrulama ve Gizlilik İhlalleri Şarj verilerndine kullanıcı kimliği , konum ve rota çıkarımı . izleme ve hedefli saldırılar için veri sızıntısı.**
15. **Ağ Katmanı DoS saldırısı EVSE/ESI/EMS iletişim kanallarının doldurulması veya radyo paraziti ile haberleşme bozulması**
16. **HSM/Kriptografik yük hedefli saldırılar HSM veya imzalama/Şifre çözme işleyicilesine aşırı yük bindirerek servis reddi veya geckme yaratmaı.**
17. **Protocoller Arası Zayıf-Nokta istismarı CAN,PLC,IP,ISO15118 ,OCPP gibi heterojen protokoller arası dönüştürücü noktarılnda veri enjeksiyonu veya kimlik doğrulama boşlukları.**
18. **ECU Zorla Durdurma Diagnostik araçlardan elde edilen CAN komutları kullanılarak motor durdurma , direksiyon ivme manipülasyonu vb gerçekleştirilebilir.**
19. **Replay Saldırısı Daha önce yakalanmış geçerli CAN çerçevelerinin tekrar gönderilmesitle yetkisiz komutların uygulanması**
20. **Truncated MAC atakları ve 32-bit MAC kırılma Riski Kısa MAC boyutu nedeniyle kaba kuvvet veya oracle tabanlı saldırı riski**
21. **Anahtar Sızıntısı / Dış cihaz aracılığıyla oturum anahtarının ele geçirilmesi Harici cihaz bağlantısının güvenliği ihlal edilirse gelecekteki oturumlar tehlikeye girebilir.**
22. **BootNotification manipülasyonu Sahte veya zamanla değiştirilmiş boot/conf mesajlarıyla CP yapılandırılmasının bozulması**
23. **SendLocaList ve LAL manipülasyonu yetkisiz ID lerin yerel yetkilendirme listesine eklenmesi(offline yetkilendirme suistimali)**
24. **RemoteStartTransaction /SetChargingProfile manipülasyonu Şarj profillerinin değiştirilmesiyle aşırı/eksik enerji teslimi**
25. **SOAP/XML özgü saldırılar : XML injection , coercive parsing , SOAP action spoofing ,WS-addressing spoofing**
26. **DoS/Coercive parsing / buffer exhaustion CS veya CP üzerinde kaynak tükenmesi**
27. **Impersonation / RFID id tag klonlama fiziksel veya mantıksal kimlik usulsüzlüğü**