Merkezi Şarj Yönetimi Üzerinden Elektrik Şebekesi İstikrarsızlığı

1. Özet

Bu senaryo, Elektrikli Araç Şarj Altyapılarının (EVCI) Merkezi Şarj İstasyonu Yönetim Sistemi (CSMS) üzerindeki zafiyetlerin istismar edilerek, binlerce yüksek güçlü şarj işleminin anlık ve senkronize bir şekilde sonlandırılmasını (toplu *RemoteStopTransaction* komutu) ele almaktadır. Bu saldırı, elektrik şebekesinden çekilen aktif yükte ani bir düşüşe (Talep Manipülasyonu) neden olarak, şebeke frekansında büyük bir sapmaya (örneğin 61.952 Hz'e) yol açma potansiyeli taşır ve bu da bölgesel elektrik kesintilerini (blackout) tetikleyebilir.

Temel anomali, siber bir kullanılabilirlik (Denial of Service, DoS) komutunun, merkezi yönetim mimarisi ve pazar tekelinin varlığı nedeniyle sistemik bir fiziksel istikrarsızlığa dönüşmesidir.

2. Amaç

Amaç, EVCI ekosisteminde taktiksel düzeyde yüksek risk taşıyan Kurcalama (Tampering, T) ve Hizmet Reddi (D) tehditlerinin, merkezi kontrol mimarisi üzerinden sistemik bir altyapı krizi boyutuna nasıl ölçeklendiğini anlamaktır. Bu çalışma, siber kontrol komutlarının kritik şebeke parametreleri (frekans ve voltaj) üzerindeki nicel etkisini analiz etmeyi ve bu yıkıcı saldırı vektörüne karşı uygulanabilir önleyici ve düzeltici stratejileri belirlemeyi amaçlamaktadır.

3. Kapsam

Bu çalışma; merkezi Şarj İstasyonu Yönetim Sistemleri (CSMS) tarafından kontrol edilen, Open Charge Point Protocol (OCPP) kullanan ve Akıllı Şebeke (Smart Grid) veya Mikroşebeke (MG) ile entegre olan Elektrikli Araç Şarj İstasyonları (EVCS) mimarisine odaklanmaktadır.

- **Dahil Olanlar:** Merkezi kontrol sistemleri (CSMS, EMS), OCPP'nin uzaktan kontrol mesajları (özellikle *RemoteStopTransaction*), ve bu komutların fiziksel şebeke üzerindeki (frekans, voltaj) etkileri.
- **Hariç Olanlar:** Doğrudan araç içi ağ (CAN Bus) saldırıları, bireysel şarj istasyonlarının fiziksel enerji hırsızlığı vakaları veya yerel düzeydeki protokol MitM (Man-in-the-Middle) saldırıları. (Ancak, bu saldırıların CSMS'e erişim sağlamak için bir Yetki Yükseltme/Elevation of Privilege vektörü olarak kullanılması kapsam dahilindedir.)

4. Tehdit Sınıflandırması

MaDEVIoT saldırısı, EVCI'deki en yüksek riskli iki STRIDE kategorisinin (T ve D) sistemik bir birleşimi olarak tanımlanır.

Kategori	Açıklama
Saldırı Tipi	Siber-Fiziksel Saldırı / Uygulama Katmanı - Kullanılabilirlik ve Bütünlük (Denial of Service / Tampering)
Kaynak Vektör	Ele Geçirilmiş Merkezi CSMS Sunucusu ve Koordineli OCPP *RemoteStopTransaction* (F03 UC) komutu.
Etkilenen Varlıklar	Kritik altyapı (Elektrik Şebekesi, Mikroşebeke), CSMS, EVCS'ler, Kontrol ve Enerji Varlıkları (c ve e).
Amaçlanan Etki	Şebeke Frekansı Sapması, Bölgesel Elektrik Kesintisi (Blackout - I-1), Hizmet Reddi (DoS) ve Kontrol Kaybı (TC-1).

5. Gerekli Koşullar (Saldırı Önkoşulları)

Bu saldırının başarılı olması ve şebeke çapında bir karartmaya yol açması için gereken kritik önkoşullar şunlardır:

- **Tek Hata Noktası Zafiyeti (Monopol/Tekel):** Saldırganın, yüksek güçte şarj yükünün kritik bir yüzdesini (örneğin %60-63) kontrol eden **tek bir merkezi CSMS sunucusunu** ele geçirebilmesi.
- **Yetki Yükseltme (EoP):** Saldırganın, merkezi CSMS sunucusuna erişim sağlayarak (örneğin Kalıcı XSS veya kimlik sahteciliği yoluyla) tüm bağlı EVCS'ler üzerinde toplu kontrol yetkisi kazanması.
- **Kamuya Açık Verilere Güven:** Saldırganların, EVCS operatörlerinin kamuya açtığı şarj yoğunluğu verilerini (Zayıf Yön) kullanarak saldırıyı şebeke yükünün en kritik olduğu ana (Tehdit) zamanlaması.
- **Protokolün Kötüye Kullanımı:** OCPP'nin RemoteStopTransaction mesajının, bireysel kullanıcı eylemi yerine toplu, senkronize bir DoS aracı olarak kötüye kullanılması.

6. Saldırı Yöntemi ve Akış

MaDEVIoT saldırısı, siber komutların fiziksel şebeke üzerindeki anlık ve yıkıcı etkisini maksimize etmeyi amaçlar.

1. **Botnet Oluşumu (Siber İhlal):** Saldırgan, bir *Elevation of Privilege (EoP)* vektörü kullanarak (örneğin, bir tedarik zinciri veya CSMS yazılım zafiyeti aracılığıyla) merkezi CSMS sunucusunu tehlikeye atar ve böylece binlerce şarj istasyonu botnet'ine erişim sağlar.
2. **Hedef Analizi (Zamanlama):** Saldırgan, şebeke operatörlerinin kamuya açık verilerini analiz ederek, aktif yükün en yüksek olduğu (Zirve Talep Penceresi) ve dolayısıyla şebekenin en hassas olduğu zamanı (örn. akşam saat 19:00) belirler.
3. **Koordineli Komut Gönderme:** Saldırgan, ele geçirdiği CSMS üzerinden, botnet'teki tüm şarj istasyonlarına eşzamanlı ve stokastik olmayan bir *RemoteStopTransaction* komutu gönderir. Bu, elektrik şebekesinden çekilen aktif yükün anlık olarak sıfırlanmasına yol açar.
4. **Fiziksel Yıkım (Frekans Sapması):** Aktif yükteki kitlesel düşüş, güç şebekesi frekansında hızlı bir artışa neden olur. Yapılan analizler, bu sapmanın frekansı **61.952 Hz** gibi operasyonel limitlerin dışına çıkarabileceğini göstermiştir. Bu anormal sapma, yerel şebekedeki **Aşırı Frekans (OF) koruma rölelerini** tetikleyerek sistem çapında bir elektrik kesintisi (blackout) başlatır.

7. Tespit Yöntemleri ve Anomali Göstergeleri

Saldırının tespiti, siber ve fiziksel katmanlardaki anormal senkronizasyonun gerçek zamanlı olarak ilişkilendirilmesini gerektirir.

Göstergeler	Açıklama
Siber Komut Anomalisi	Tek bir merkezi kaynaktan (CSMS) gelen, insan/ekonomik mantıkla korelasyon göstermeyen, **yüksek hacimli ve senkronize** *RemoteStopTransaction* mesajlarının akışı.
Fiziksel Frekans Anomalisi	Güç şebekesi frekansında, operasyonel limitlerin (örn. 60 Hz) ötesinde ani ve anormal **Yükselme Hızı (RoC)** tespiti (örneğin, 61.952 Hz tepe noktası).
Mantıksal Korelasyon Anomalisi	Siber olay (toplu şarj kesme) ile fiziksel olay (frekans yükselmesi) arasında düşük gecikmeli, **anlamsız bir korelasyonun** tespiti.
Davranışsal Anomali (Botnet)	Öğrenilmiş normal kullanıcı profillerine kıyasla, *Transaction* sonlanma desenlerindeki ani ve kitlesel sapmaların tespiti.

8. Önlemler ve Azaltma Stratejileri

Azaltım stratejileri, sistemin merkezi zafiyetini (Tek Hata Noktası) gidermeye ve Kurcalama/Hizmet Reddi (T/D) risklerini ortadan kaldırmaya odaklanmalıdır.

Alan	Aksiyon	Etkilediği Kritik Risk (T, D)
Mimari Dayanıklılık	Merkezi CSMS'e bağımlılığı azaltan **Dağıtık Kontrol Algoritmalarının** (Distributed Control Algorithms) uygulanması.	D (Sistemik çöküş)
Protokol Sertleştirme	OCPP iletişimlerinde MitM ve Kimlik Sahteciliğini önlemek için **Karşılıklı TLS (Security Profile 3)** ve **IPSec** zorunluluğu.	T, D, S, E
Veri Bütünlüğü	Tüm kritik komutlar ve sayaç değerleri için (örn. *RemoteStopTransaction*) **Dijital İmza (MAC/Hash)** zorunluluğu.	T, R (Kurcalama, İnkar)
Anomali Tespit (IDS)	Siber (komut senkronizasyonu) ve Fiziksel (frekans RoC) verileri gerçek zamanlı olarak ilişkilendirebilen **ML/AI tabanlı ADS** sistemlerinin konuşlandırılması.	D, T
Fiziksel Güvenlik	Genel kullanıma açık istasyonlarda (CS) fiziksel manipülasyonu önlemek için **darbeye dayanıklı kasalar** ve **yazılım tabanlı anti-kurcalama** çözümleri.	T, S

9. Sonuç

Bu anomali senaryosu, yüksek güçlü EVCI'lerin, özellikle V2G (Araçtan Şebekeye) teknolojisinin yaygınlaşmasıyla birlikte, basit bir IoT zafiyetinin ulusal altyapı güvenliğine yönelik en yüksek risklerden biri haline geldiğini kanıtlamaktadır. Siber risklerin en çok Kurcalama (T - 8.6) ve Hizmet Reddi (D - 9.2) kategorilerinde yoğunlaşması, gelecekteki güvenlik mimarilerinin sadece şifrelemeye değil, aynı zamanda **merkeziyetçilik sorununu çözen** Dağıtık Kontrol ve **gerçek zamanlı korelasyona dayalı davranışsal anomali tespitine** odaklanması gerektiğini göstermektedir.