□ Akıllı Şarj İstasyonu

Anomali Senaryosu: Enerji Ölçüm Sapması – Sayaç Kalibrasyon Manipülasyonu

Özet

Bu anomali, şarj istasyonundaki enerji ölçüm (Smart Meter) cihazının kalibrasyon verilerinin yetkisiz biçimde değiştirilmesiyle ilgilidir. Amaç, istasyonun ölçtüğü tüketimi olduğundan düşük veya yüksek göstermektir. Bu durum doğrudan gelir kaybı, hatalı faturalandırma ve yasal yükümlülük ihlali doğurur. Saldırgan fiziksel erişim (servis portu, RS-485 hattı) veya bakım modundaki bir açık aracılığıyla ölçüm katsayısını (örneğin scale_factor) değiştirir. Bu değişiklik yazılımsal loglarda görünmez, ancak CSMS tarafında faturalama anomalisi oluşur.

1. Normal İşleyiş

1. Araç bağlanır, CS ile CSMS arasında BootNotification, Authorize ve StartTransaction mesajları ile kimlik doğrulama yapılır. 2. Smart Meter, energyWh değerini periyodik olarak gönderir. 3. CSMS bu veriyi toplar, faturalandırma birimi olarak kullanır. 4. Ölçüm katsayısı fabrika kalibrasyonuna göre sabittir (örneğin 1.0000).

2. Anomali: Kalibrasyon Değeri Manipülasyonu

Saldırgan, servis bağlantı portuna erişir veya Maintenance API üzerinden MeterCalibration parametresine sahte değer yazar. Örneğin, scale_factor 1.0000 yerine 0.85 yapılır. Sonuç: sistem, 10 kWh yerine 8.5 kWh tüketim raporlar.

3. Saldırı Aşamaları

- Keşif: Saldırgan, istasyon yazılım sürümünü ve modbus portlarını tespit eder.
- Yetkisiz Erişim: Bakım portu (ör. RS-485 veya Modbus TCP) şifre korumasızdır.
- Parametre Değiştirme: Saldırgan, Meter Scaling veya Calibration Offset parametresini değiştirir.
- Normal Operasyon: CSMS tarafında her şey normal görünür; ancak gerçek tüketimle raporlanan değer arasında fark oluşur.
- Tespit Edilmediği Durumda: Uzun süreli gelir kaybı ve regülasyon ihlali meydana gelir.

4. Teknik Etkiler

• Faturalandırma Sapması: %10–20’ye varan yanlış ölçüm. • Enerji Kaçak Riski: Gerçek tüketim raporlanandan yüksek. • Raporlama Hatası: Kurumlararası enerji denetimlerinde veri tutarsızlığı. • Yasal Risk: Ölçüm cihazı kalibrasyon sertifikasının geçersiz sayılması.

5. Algılama Mantığı

• Çapraz Ölçüm: Smart Meter ile harici sayaç karşılaştırılır. • Trend Analizi: Geçmiş 7 gün ortalamasıyla % fark > 8 ise alarm. • Firmware Hash Kontrolü: Ölçüm modülünün

checksum değeri farklıysa uyarı. • Parametre İzleme: scale_factor ve calibration_date değişmişse log kaydı tetiklenir.

6. Karar ve Müdahale

Şüphe: İstasyonun faturalandırması geçici olarak durdurulur. İnceleme: Uzaktan “Calibration Audit” isteği gönderilir. Onaylı Anomali: Ölçüm cihazı devre dışı bırakılır, manuel sayaç verisiyle dengeleme yapılır. Kurtarma: Kalibrasyon verisi üretici imzasıyla yeniden yüklenir.

7. Örnek Loglar

2025-11-03T21:14:01Z | StationID: ST-225 | Event: CalibrationParamChanged | scale_factor: 0.85 | Operator: unknown | Action: FlaggedForAudit
2025-11-03T21:15:12Z | StationID: ST-225 | Event: BillingAnomalyDetected | expected: 10.00 kWh | reported: 8.47 kWh | Action: AuditTriggered 2025-11-03T21:18:09Z | StationID: ST-225 | Event: RemoteCalibrationRestored | scale_factor: 1.00 | Action: NormalOperationResumed

8. Teknik Nedenler

• Bakım portu veya servis API’sinde kimlik doğrulama eksikliği. • Kalibrasyon parametrelerinin şifrelenmeden saklanması. • Firmware’in immutable configuration koruması bulunmaması. • Denetim sistemiyle sayaç arasındaki veri bütünlüğü eksikliği.

9. Etkiler

• TC-5 / TC-7: Yanlış fatura / gelir kaybı. • I-3: Güven ve regülasyon riski. • R-1: Tedarikçi sorumluluğu ihlali (yasal yükümlülük).

10. Öneriler

1. Immutable Calibration Zone: Kalibrasyon parametreleri salt-okunur bölgede saklanmalı. 2. Maintenance Port Authentication: Servis erişimi çift faktörlü olmalı. 3. Hash-based Audit: Her MeterValues gönderiminde ölçüm modül hash’i eklenmeli. 4. Çapraz Doğrulama: İstasyon belirli aralıklarla şebeke ölçüm verisiyle eşleştirilmeli. 5. SOC / SIEM Kuralı: CalibrationParamChanged olaylarını gerçek zamanlı yakalayacak alarm tanımlanmalı. 6. Regülasyon Uyumu: Ölçüm cihazları yılda en az bir kez akredite kuruluş tarafından yeniden kalibre edilmeli.

11. Referanslar

• OCPP 2.0.1 Specification – Metering and Calibration Security Section • ENISA (2024): Integrity Attacks in Smart Energy Systems • IEEE Access (2023): Tamper-Resistant Meter Calibration Methods • ScienceDirect (2025): Secure Modbus Communication in EV Infrastructure