MeterValues Yeniden Ataması ile Haksız Faturalama ve Veri Bozması

Tarih: 29.10.2025

Hazırlayan:Kevser Aslan

Amaç: Şarj oturumu verilerini ele geçirip (transactionId / idTag) MeterValues kayıtlarını başka bir hesaba yeniden atamak veya kayıtlardan gizleyerek haksız faturalandırma ve veri tutarsızlığı yaratmaktır.

Senaryo Özeti: Ne Oluyor?

Saldırgan, şarj oturumuna ait **transactionId** veya **idTag** bilgilerine yetkisiz erişim elde ederek (çalışan kimlik bilgisi, çalıntı API tokenı veya zayıf admin kontrolleri aracılığıyla) merkezi yönetim sistemindeki (CSMS) oturum kayıtlarını değiştirir. Bu erişimle saldırgan; mevcut MeterValues girişlerini başka bir kullanıcı hesabına atayabilir, bazı MeterValues kayıtlarını iletmeyerek kayıtlardan silebilir veya sampledValue değerlerini doğrudan değiştirebilir. Sonuç olarak fiziksel sayaç doğru enerji ölçümünü yaparken merkezi sistemde görünen kayıtlar farklı hesaplara yazılır veya eksik/yanlış raporlanır; bu durum haksız faturalandırma, operatör gelir kaybı ve şebeke yönetiminde hatalı kararlar doğurur.

Saldırı Mekanizması: Nasıl Yapılır?

Yönetici / Operatör Yetkilerinin Ele Geçirilmesi (Doğrudan Reassignment)

1. Saldırgan, sosyal mühendislik (phishing), credential stuffing veya bir insider yardımıyla CSMS yönetici/operatör hesabını veya yetkili bir servis hesabını ele geçirir.
2. Yönetici paneli veya yetkili API aracılığıyla aktif transaction listesine erişir ve hedef transactionId/connectorId/idTag bilgilerini belirler.
3. Hedef transaction üzerindeki MeterValues kayıtlarını seçer ve idTag veya transactionId alanlarını başka bir kullanıcıya/hesaba (ör. saldırgana ait veya sahte bir hesap) yeniden atar; ya da seçili MeterValues kayıtlarını veritabanından siler.
4. Değişiklikler CSMS veritabanında onaylanır; faturalama ve raporlama modülleri bu manipüle edilmiş veriler üzerinden sonuç üretir.
5. Saldırgan gerektiğinde eski kayıtları (audit log) gizlemeye veya değiştirmeye çalışır.

Örn: Admin hesabı ile 2025-11-02 08:00'da başlayan transactionId=1234 içindeki üç MeterValues kaydı farklı bir idTag=ATTACKER_TAG ile ilişkilendirilir; sonuç olarak gerçek kullanıcı fatura ödemezken saldırgan hesabına faturalama düşer.

API Token Sızıntısı / Zayıf API Yetkilendirme (Uzaktan Script ile Toplu Yeniden Atama)

1. Saldırgan, kamusal veya zayıf korunan CSMS API uç noktasından sızdırılmış bir token veya zayıf konfigüre edilmiş bir servis hesabı bulur (ör. token uzun süre geçerli, scope geniş).
2. Otomatik bir script ile CSMS API'sine bağlanarak aktif transaction'ları tarar ve hedef transactionId/uniqueId/connector bilgilerini listeler.
3. Script, hedef kayıtların transactionId veya idTag alanlarını PATCH/PUT isteğiyle programatik olarak değiştirir (reassignment) veya MeterValues endpoint'ine sahte, düşük değerli sampledValue gönderir.

4. Değiştirilen kayıtlar hemen raporlama/ faturalama pipeline'ına akar; saldırgan istenirse birden fazla istasyon için aynı işlemi topluca uygular.
5. Eğer SignedMeterValues gibi imza denetimleri yoksa veya yetersizse değişiklikler kolayca kabul edilir; logging ise zayıfsa silme/örtme adımları da yapılabilir.

Örn: Sızdırılmış API token ile gece 02:00–03:00 arası 200 aktif transaction için otomatik script çalıştırılarak sampledValue %60 oranında azaltılır; operatörün günlük gelir raporu önemli ölçüde düşer.

(Alternatif/Yardımcı) Yöntem: İçeriden Veri Değiştirme / Veritabanı Seviyesinde Manipülasyon

1. Saldırgan doğrudan CSMS veritabanına erişim elde etmişse (SQL injection, leaked DB creds veya insider), MeterValues tablolarındaki idTag/transactionId/sampledValue sütunlarını doğrudan günceller.
2. Bu yöntem değişikliklerin çok hızlı ve kapsamlı yapılmasını sağlar; ancak başarılı olursa detection zorluğu artar çünkü değişiklikler uygulama seviyesinden değil veri seviyesinden gelir.

Örn: DB erişimi ile bir gece yarısı 10.000 kayıt üzerinde sampledValue = sampledValue * 0.5 güncellemesi yapılır; günlük faturalama raporu ciddi sapma gösterir.

Saldırı Neden Başarılı Olur?

Eksiklik	Açıklama
Zayıf yönetici koruması	MFA/yöneticı kontrolleri yok → hesap ele geçirilebilir.
Sızdırılmış/uzun ömürlü API token	Token ile toplu yeniden atama yapılabilir.
Mesaj imzası yok	MeterValues dijital imza içermiyorsa değişiklik tespit edilemez.
Transaction-binding yok	Start/Stop oturumları kriptografik bağlanmamış, yeniden atama kolay.
Zayıf logging / immutable kayıt yok	Yapılan değişiklikler loglardan silinebilir.
Yetersiz anomali izleme	Toplu manipülasyonlar erken fark edilmez.

Riskler ve Zararlar :

Kategori	Etkilenen Alan
Finansal	**Gelir Kaybı:** Operatör, yeniden atanmış/eksik kayıtlardan dolayı ciddi gelir kaybına uğrar. **Haksız Faturalandırma:** Müşteriler yanlış veya eksik faturalandırılabilir; iade ve itiraz maliyetleri artar.
Operasyonel	**Bozulan Raporlama:** Şebeke yük tahminleri ve kapasite planlaması hatalı veri yüzünden yanlış yapılır. **İş Sürekliliği:** Faturalama/işlem hata oranı artarsa operasyonel yük yükselir.
Gizlilik	**Kişisel Veri Sızıntısı:** idTag/kimlik eşleştirmeleri kötüye kullanılırsa kullanıcı bilgilerinin açığa çıkması söz konusu olabilir.
İtibar	**Müşteri Güveni Zedelenir:** Yanlış faturalar ve veri güvenliği ihlalleri marka itibarına zarar verir, müşteri kaybı yaşanır.
Yasal / Uyumluluk	**Mevzuat İhlali:** Fatura doğruluğu ve veri bütünlüğü ile ilgili yasal düzenlemeler (KVKK/MID vb.) ihlal edilebilir; ceza ve tazminat riski doğar.

Tespit Yöntemleri (Saldırı Olduysa):

1. **Transaction–ID Tutarlılık Kontrolü:** Aynı transactionId için idTag değişimi veya kısa sürede tekrar atama tespit edilirse alarm ver.
2. **MeterValues ↔ Fiziksel Sayaç Karşılaştırması:** Raporlanan MeterValues ile fiziksel sayaç/gateway verisi arasındaki fark %10'dan fazla ise uyarı üret.
3. **Admin / API Aktivite Anomalileri:** Yönetici hesaplarından veya API token ile yapılan toplu PATCH/PUT çağrılarında olağan dışı hız/dağılım varsa (ör. 1 dk içinde 50+ reassignment) kırmızı alarm.
4. **Olay Zamanlaması İzlemesi:** Yönetici işlemleri mesai dışı (gece) veya kısa aralıklarla yapılıyorsa risk göstergesi.
5. **Sıra / Replay Kontrolü:** uniqueId veya sequence numarası tekrarı, gap veya geri sarma varsa "replay / manipulation" alarmı.
6. **İmzalama Durumu Kontrolü:** Gelen MeterValues'ta signature_status başarısızsa ya da imza eksikse kayıt reddi ve uyarı.
7. **Toplu Anomali Tespiti (ML):** Her idTag için normal profil (ortalama kWh, süre, frekans) öğrenilip, büyük sapmalar (örn. ±%30) ML ile işaretlensin.
8. **SIEM Korelasyonu:** Yönetici oturumu açma + aynı anda veri değişikliği + IP coğrafya değişimi gibi birden fazla sinyal birleşince yüksek öncelikli olay oluştur.
9. **Audit Log Tutarsızlığı Kontrolü:** Loglarda sıra boşlukları veya silinmiş zaman damgaları tespit edilirse olay başlat.
10. **Kullanıcı Şikayeti İzleme:** Aynı bölgeden gelen fatura itirazları artıyorsa otomatik inceleme tetikle.

Savunma Mekanizmaları:

Katman	Savunma Mekanizması
Kimlik & Erişim	MFA, rol bazlı erişim (RBAC) ve yönetici işlemleri için çift onay.
API Güvenliği	Kısa ömürlü token, IP kısıtlaması ve rate-limit uygulanması.
Veri Bütünlüğü	MeterValues kayıtlarının dijital imzalanması (SignedMeterValues).
Kayıt & İzleme	Değiştirilemez loglar (immutable) ve düzenli anomali analizi.
Çapraz Doğrulama	Fiziksel sayaç verisi ile merkezi sistem verisinin periyodik karşılaştırılması.

SWOT Analizi: Transaction Yeniden Atama ve MeterValues Manipülasyonu

S STRENGTHS	W WEAKNESSES	O OPPORTUNITIES	T THREATS
• Gerçek siber tehdit senaryosu (veri manipülasyonu) üzerine kuruludur. • Veri bütünlüğü ve kimlik doğrulama eksikliklerini vurgular. • Makine öğrenmesiyle tespit edilebilir bir yapı sunar.	• Saldırı verisel düzeyde gerçekleştiği için tespiti zordur. • Gerçek saha verisine erişim olmadan test sınırlı olabilir. • Model yanlış pozitif sonuçlar üretebilir.	• Yeni güvenli OCPP protokolleri için öneriler geliştirilebilir. • Gerçek zamanlı faturalama doğrulama sistemleri için temel oluşturur. • Endüstriyel iş birlikleri ve akademik araştırma fırsatları sağlar.	• Saldırganlar yeni teknikler geliştirebilir. • Yetersiz yatırım yapılırsa tehdit uzun vadede devam eder. • Veri sızıntısı yasal ve finansal risk oluşturabilir.