Anomali Senaryosu

İmzalı MeterValues Replay ve Zaman Damgası Manipülasyonu — Signed MeterValues Replay with Timestamp Manipulation

Özet

Saldırgan, CS (Charging Station) ile CSMS arasındaki imzalanmış MeterValues mesajlarını yeniden oynatır (replay) veya zaman damgasını değiştirir; böylece gerçek enerji tüketimi gizlenir ya da yanlış/tekrarlı ölçümler oluşur. Sonuç: hatalı faturalandırma (eksik veya çift), SmartCharging kararlarının bozulması ve settlement/raporlama hataları.

Ön Koşullar

• CS MeterValues gönderiyor ve imzalı MeterValues seçeneği etkin ya da opsiyonel olarak mevcut.

• Saldırgan, trafiği yakalayabilecek (MitM) veya önceden kaydedilmiş MeterValues paketlerine erişebilecek konumda.

• CSMS, zaman sırası/nonce doğrulaması veya monotonicity kontrolleri olmadan imzalı MeterValues'ı fatura için kabul ediyor.

Senaryo Adımları

1) Normal Başlangıç: Araç bağlanır, StartTransaction çalışır; CS periyodik olarak MeterValues (energyWh, timestamp, signature) gönderir. CSMS bu değerleri tutar.

2) Paket Kayıt/İzleme: Saldırgan ağ trafiğini kaydeder veya geçmiş oturum MeterValues örneklerini elde eder.

3) Zaman Damgası Manipülasyonu / Replay: Saldırgan aynı MeterValues paketlerini yeniden gönderir veya timestamp'ı değiştirerek farklı bir zaman penceresine yerleştirir; bazen paketler birden çok kez gönderilir.

4) Sonuç: CSMS, eğer sıralama/monotonicity kontrolü yapmıyorsa; ya tüketimi düşük gösterir (eksik fatura) ya da aynı değerleri iki kez sayar (çift faturalandırma). EMS/SmartCharging yanlış karar alabilir.

Algılama Mantığı

• İmza doğrulama: Signature ve certificate geçerliliği kontrolü (CRL/OCSP).

• Monotonik Kontrol: Her transactionId için energyWh değerinin artan olması gerekir; düşüş veya tekrar tespit edilirse uyarı.

• Zaman Damgası Tutarlılığı: Büyük geri dönüşler veya tutarsız zaman sıçramaları incelenir.

• Nonce/Challenge Kullanımı: CSMS tarafından üretilen nonce'un imza içinde yer alması gerekir; yoksa replay şüphesi.

• Cross-validation: Donanımsal sayaç (smart meter) veya başka güvenilir kaynaklarla kıyaslama.

Karar ve Müdahale

• Şüphe halinde: MeterValues 'suspect' olarak işaretlenir; faturalama askıya alınır; CS'den nonce-challenge istenir.

• Güçlü kanıt: Oturum 'inconsistent' olarak işaretlenir; ilgili MeterValues kayıtları faturalamadan çıkarılır; manuel reconciliation başlatılır.

• Saldırı kanıtlanırsa: Bağlantı engellenir; ilgili sertifikalar incelenir/iptal edilir; SOC'a bildirim gönderilir; adli/teknik inceleme başlatılır.

Örnek Loglar

2025-11-03T09:12:01Z | StationID: ST-112 | TxID: TR-9981 | Event: MeterValuesReceived | energyWh: 120400 | ts: 2025-11-03T08:59:58Z | signature: VALID | Action: PendingMonotonicityCheck

2025-11-03T09:12:05Z | StationID: ST-112 | TxID: TR-9981 | Event: MeterValuesReceived | energyWh: 120400 | ts: 2025-11-03T03:00:00Z | signature: VALID | Action: ReplaySuspected; Flagged; RequestNonceChallenge

2025-11-03T09:12:10Z | StationID: ST-112 | TxID: TR-9981 | Event: NonceChallengeSent | nonce: N-7G4H2 | Action: AwaitingSignedMeterValue

2025-11-03T09:12:22Z | StationID: ST-112 | TxID: TR-9981 | Event: MeterValuesReceived | energyWh: 120560 | ts: 2025-11-03T09:12:20Z | signature: VALID (includes nonce N-7G4H2) | Action: Accepted; Reconciled

Teknik Nedenler

• Nonce veya sequence kontrolü olmadan imzalı veri kabulü.

• Zayıf ağ güvenliği ve MitM olanağı.

• CS ile CSMS arasında saat senkronizasyonu (time sync) sorunları.

• Faturalama sisteminin tek imzalı packet'a dayanması ve toplulaştırma/detaylı doğrulamayı atlaması.

Etkiler

• TC-3 / TC-7 / TC-4: Hatalı faturalandırma (ekonomik kayıp), enerji hırsızlığı, veri güvenine zarar.

• I-3 ve I-4: Ekonomik zarar ve itibar/konfidansiyalitenin zedelenmesi.

Öneriler

1. Nonce-based Signed MeterValues: CSMS nonce'u imzalanan veri içinde zorunlu hale getirilmeli.

2. Sequence & Monotonic Checks: Her TxID için energyWh artışı zorunlu kontrol edilmelidir.

3. Zaman Senkronizasyonu: NTP/PTP kullanımı ve drift izleme.

4. Sertifika Kontrolü: CRL/OCSP ile anlık iptal ve geçerlilik kontrolü.

5. Raw Packet Store: Delil amaçlı ham paketlerin saklanması.

6. Cross-validation: Donanımsal sayaç kıyaslaması.

7. SOC/EDR Kuralları: Replay ve timestamp anormalliklerini yakalayan kural setleri.

8. Replay Window Limits: Belirli bir zaman penceresinden eski MeterValues reddedilsin.

Referanslar

• OCPP 2.0.1 Specification — MeterValues & SignedMeterValues

• Araştırmalar: Replay Attacks ve Time Manipulation in CPS / SmartMeters