OCPP Oturum Bilgilerinin Ele Geçirilmesi – Veri Gizliliği İhlali (Protokol Güvenlik Açığı)

1. Anomali Tanımı

OCPP protokolü, şarj istasyonları ile arka uç yönetim sistemleri arasında enerji tüketimi, zamanlama ve fiyatlandırma gibi işlemlerin koordinasyonunu sağlar.
Bu kapsamda **enerji ölçüm verileri** (meterValue), **şarj seansı detayları**, **kimlik bilgileri** ve **şarj başlangıç/bitiş zamanları** merkezi sistemlere iletilir.

Ancak bu veriler şifrelenmeden ya da doğrulama mekanizmaları olmadan iletildiğinde, saldırganlar veya yetkisiz kişiler bu bilgileri değiştirerek:

- Fatura tutarlarını manipüle edebilir,
- Tüketimi düşük gösterebilir,
- Başka bir kullanıcının oturumunu taklit ederek ücretsiz şarj alabilir.

Bu açıklar, doğrudan **gelir kaybına**, **işletme operasyonlarının bozulmasına** ve **müşteri güveninin sarsılmasına** neden olabilir.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama
Kategori	**Olası Sebep**	**Açıklama**
Protokol	Veri bütünlüğü kontrol eksikliği	Gönderilen sayaç ve zaman verileri dijital olarak imzalanmaz veya doğrulanmaz.
Uygulama	İstemci taraflı sayaç verisine güvenilmesi	İstasyonun gönderdiği ölçüm verisinin merkezi sistem tarafından sorgusuz kabul edilmesi.
Ağ Katmanı	Şifreleme veya TLS kullanılmaması	Veriler açık metin iletildiğinde üçüncü taraflar tarafından değiştirilebilir.

3. Olası Riskler ve Etkiler

- Sayaç verilerinin eksik veya yanlış gösterilmesi sonucu **düşük veya sıfır fatura** oluşması
- **Kullanıcının başka birinin oturumunu taklit etmesiyle ücretsiz şarj yapması**
- Zaman bazlı tarifelerde oturum sürelerinin manipüle edilmesi
- Yanlış faturalama nedeniyle **müşteri şikayetleri ve destek taleplerinin artması**
- **Toplu gelir kaybı** ve muhasebe sistemleriyle uyumsuzluk
- **İşletmenin itibarı ve kullanıcı güveninin zedelenmesi**

4. İlgili Standart / Referans

- **OCPP 1.6 / 2.0.1 Specification** – Open Charge Alliance
- **ISO 15118-2** – EV-EVSE güvenli iletişim ve ödeme sistemi entegrasyonu
- **IEC 62053 / 62056** – Elektrik sayaçları için ölçüm doğruluğu ve veri aktarımı
- **ISO 27001** – Bilgi güvenliği yönetimi
- **OWASP Top 10** – Integrity violation (Broken data validation)

5. Çözüm Önerileri (kolay uygulanabilir, maddeler halinde)

Yazılım Düzeyinde:

Uygulama Katmanında:

- Sayaç verilerinin güvenilir kaynaklardan geldiği doğrulanmalı
- Her oturum, şarj başlangıcı, bitişi ve sayaç bilgileri dijital olarak imzalanmalıdır
- Oturum açma ve bitirme komutları için kullanıcıya özel kimlik doğrulama uygulanmalıdır

Protokol / Ağ Düzeyinde:

- Tüm OCPP mesaj trafiği TLS 1.2+ protokolü ile şifrelenmelidir
- Mutual TLS (çift taraflı doğrulama) ile sadece yetkili cihazların bağlantısına izin verilmelidir

Operasyonel Önlemler:

- Faturalama verileri için merkezi sistemde ek bütünlük kontrolleri yapılmalı
- Otomatik raporlar ve eş zamanlı sayaç uyuşmazlık kontrolleri devreye alınmalıdır
- Şüpheli oturum veya sayaç verisi değişikliği tespitinde sistem yöneticileri uyarılmalıdır

6. Sonuç ve Değerlendirme

Faturalama verilerinin ve oturum bilgilerinin dış müdahaleye açık olması, hem bireysel kullanıcılar hem de şarj ağı operatörleri için **doğrudan maddi kayıplar** anlamına gelir.
Bu açık, operasyonel istikrarı bozar, müşteri güvenini sarsar ve yasal/finansal yükümlülükler doğurur.

Dolayısıyla, bu açıklık **kritik önemde** olup güvenli yazılım mimarisi, veri bütünlüğü kontrolü ve şifreli iletişim yöntemleriyle mutlaka giderilmelidir.

.

7. Kaynaklar

Open Charge Alliance. (2020). *OCPP 2.0.1 Specification*. Open Charge Alliance. (2020). *OCPP 2.0.1 Specification*. [https://www.openchargealliance.org/]

ISO 15118-2 – *Vehicle to Grid Communication Interface*

IEC 62053-21 / 62056 – *Electricity metering equipment protocols*

OWASP – *Broken Data Validation and Injection*

B. Zimmermann et al. (2021). *Security Analysis of Electric Vehicle Charging Protocols*, Springer