IEC 61851 İletişim Kesintisi – Enerji Akışı Devam Ediyor (Protokol Uyum Anomalisi)

1. Anomali Tanımı

Elektrikli araç şarj altyapısında kullanılan OCPP protokolü, sadece oturum başlatma/durdurma işlemleriyle sınırlı değildir. Protokol aynı zamanda:

- Maksimum akım değerinin ayarlanması (SetChargingProfile),
- Şarj konfigürasyonlarının değiştirilmesi (ChangeConfiguration),
- Donanım resetleme (Reset),
- Yazılım güncellemesi başlatma gibi komutlar içerebilir.

Bu komutların **yetkisiz kişiler tarafından gönderilmesi veya manipülasyonu**, sistemin fiziksel bileşenleri üzerinde doğrudan etkiler yaratabilir. Örneğin, yanlış konfigürasyon ile:

- Aşırı akım gönderilebilir,
- Soğutma sistemleri devre dışı kalabilir,
- Şarj durumu bozulabilir.

Bu durumlar, **yangın, batarya hasarı veya elektrik altyapısı arızalarına** yol açabilecek ciddi **güvenlik riskleri** doğurur.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama
Kategori	**Olası Sebep**	**Açıklama**
Protokol	Komutların kriptografik doğrulamasının olmaması	Gelen komutlar şifrelenmeden veya imzalanmadan kabul edilebilmektedir.
Yazılım	Komut filtreleme ve izin denetimi eksikliği	İstasyon kontrol yazılımı, tüm komutlara açık yapıdadır; yetkili mi kontrol edilmez.
Ağ	TLS olmayan haberleşme	Saldırgan, araya girerek komutları değiştirebilir ya da kendi komutlarını enjekte edebilir.

3. Olası Riskler ve Etkiler

- Aşırı yüksek akım sınırı belirlenerek **batarya sistemine fiziksel zarar verilmesi**
- Soğutma sistemlerinin devre dışı bırakılması yoluyla **ısınma ve yangın riski oluşması**
- Reset komutlarının sürekli gönderilmesiyle **cihazın arızaya zorlanması**
- DC hızlı şarj sırasında akım/frekans bozulmaları sonucu **şebekeye zarar verilmesi**
- **Kritik elektrik güvenlik korumalarının (örneğin topraklama, aşırı akım) baypas edilmesi**

4. İlgili Standart Referansı

- **IEC 61851-1 / -23 / -24** – EVSE elektriksel güvenlik gereksinimleri
- **OCPP 2.0.1 Functional Specification** – Open Charge Alliance
- **ISO 26262** – Functional Safety for Road Vehicles
- **IEC 62196** – Şarj donanımı ve konnektör güvenliği
- **SAE J2931** – Electric Vehicle Communication Security

5. Çözüm Önerileri

Protokol Düzeyinde:

- OCPP 2.0.1 veya üstü sürümlerine geçiş yapılmalı; bu sürümler TLS ve mesaj imzalama desteği sunar.
- Kritik komutlar için ilave doğrulama (örn. çift faktör, yetki derecesi) uygulanmalıdır.

Yazılım Düzeyinde:

- Şarj cihazı yalnızca güvenilir merkezi sunucudan gelen komutları kabul etmelidir.
- Komutların içeriği ve bağlamı analiz edilerek olağandışı talepler reddedilmelidir (ör. 500A akım limiti).

Güvenlik Testi / İzleme:

- Komut trafiği sürekli olarak log'lanmalı ve analiz edilmelidir.
- Güvenlik duvarı ve IDS/IPS sistemleri OCPP komut manipülasyonlarına karşı yapılandırılmalıdır.
- Komut seviyesinde test senaryoları oluşturularak cihaz davranışı gözlemlenmelidir.
    - .

6. Sonuç ve Değerlendirme

Şarj sistemleri yalnızca bilgi işlem altyapısı değil, aynı zamanda yüksek güçlü elektrik donanımlarını içerir. Bu nedenle, kritik komutlara yetkisiz erişim yalnızca sistem hatasına değil, **fiziksel zararlara** ve **can güvenliği tehlikesine** yol açabilir.

Bu güvenlik açığı; "yüksek riskli güvenlik-kritik anomali" olarak sınıflandırılmalı, üretimden önceki test süreçlerinde mutlaka değerlendirilmelidir.

.

7. Kaynakça

- Open Charge Alliance. (2020). *OCPP 2.0.1 Functional Specification*. [https://www.openchargealliance.org/]
- IEC 61851-1 / -23 / -24 – *Electric Vehicle Conductive Charging Systems*
- ISO 26262 – *Road Vehicles – Functional Safety*
- SAE J2931 – *Digital Communication for Electric Vehicle Charging*
- R. Khera et al. (2021). *Electric Vehicle Charging Infrastructure Security: Threats and Solutions*, IEEE Acces