OCPP Komutlarının Yetkisiz Kullanımı – Hizmet Kesintisi ve Hatalı Konfigürasyon (Protokol Güvenlik Açığı)1. Anomali Tanımı

1. Anomali Tanımı

Open Charge Point Protocol (OCPP), elektrikli araç şarj istasyonlarının merkezi sistemlerle haberleşmesini sağlayan yaygın bir protokoldür.
OCPP üzerinden gönderilen kritik komutlar arasında **RemoteStartTransaction**, **RemoteStopTransaction**, **Reset**, **ChangeConfiguration** gibi işlemler yer alır.

Bu komutların gönderimi sırasında kimlik doğrulama ya hiç yapılmamakta ya da zayıf şekilde uygulanmaktadır.
Bu durum, yetkisiz bir saldırganın bu komutları taklit ederek şarj işlemlerini kesintiye uğratmasına veya sistem yapılandırmasını değiştirmesine neden olabilir.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama
Kategori	Olası Sebep	Açıklama
Protokol	OCPP kimlik doğrulama eksikliği	OCPP 1.6 sürümü ve öncesinde kimlik doğrulama zorunlu değildir.
Yazılım	Komut yetkilendirme kontrolünün eksikliği	Backend sunucusu her komutun kimden geldiğini ve geçerli olup olmadığını doğrulamayabilir.
Ağ	TLS veya güvenli kanal eksikliği	Mesajlar şifrelenmeden iletildiğinde araya girilerek değiştirilebilir.

3. Olası Riskler ve Etkiler

- **Şarj işleminin izinsiz durdurulması** → Müşteri hizmeti kesintiye uğrar.
- **Yanlış güç limiti ayarlanması** → Aşırı yükleme veya şarj hızının düşmesi.
- **İstasyonda dengesiz davranışlar** → Konfigürasyonların hatalı değişmesi sonucu cihaz hataları.
- **Müşteri memnuniyetsizliği** → Güvensiz hissetme, destek talepleri, marka itibar kaybı.

4. İlgili Standart / Referans

- **OCPP 1.6 & 2.0.1 Specification** – Open Charge Alliance
- **IEC 61851-24** – EV şarj donanımı ve iletişim katmanı
- **ISO 15118** – Plug & Charge, kimlik doğrulama katmanı
- **OWASP** – Broken Authentication and Access Control riskleri

5. Çözüm Önerileri (kolay uygulanabilir, maddeler halinde)

Yazılım Düzeyinde:

- Komut bazlı **yetkilendirme (authorization)** sistemi uygulanmalı.
- Komut gönderen her istemci, sistemde tanımlı kullanıcı/operatör olmalı.
- Her işlem audit log'lara kaydedilmeli.

Ağ Katmanında:

- **TLS 1.2 veya 1.3** üzerinden şifreli bağlantılar zorunlu hale getirilmeli.
- Sertifika tabanlı istemci doğrulama (mutual TLS) kullanılmalı.

Test Aşamasında:

- Penetrasyon testlerinde "unauthorized RemoteStop" gibi senaryolar simüle edilmeli.
- SIEM sistemleri ile kötüye kullanım davranışı tespit edilmeli.

6. Sonuç ve Değerlendirme

OCPP komutlarının yetkisiz şekilde gönderilmesi, şarj hizmetinin sürekliliğini ve güvenilirliğini doğrudan etkileyen **yüksek öncelikli bir açıklıktır**.
Bu açık, yalnızca bireysel kullanıcıları değil, aynı anda binlerce şarj noktası işleten ağları da etkileyebilir.

Bu nedenle tüm OCPP uygulamalarında kimlik doğrulama ve komut yetkilendirme **zorunlu güvenlik gereksinimleri** olarak uygulanmalı; ilgili sistemler düzenli olarak denetlenmelidir

.

6. Kaynaklar

- Open Charge Alliance. (2020). *OCPP 2.0.1 Specification*. https://www.openchargealliance.org/
- IEC 61851-24 – *Digital Communication between DC EVSE and EV*
- OWASP Foundation – *Top 10 Web Application Security Risks*
- M. Stelios et al. (2023). *Survey on OCPP Security Issues*. arXiv:2207.01950
- Rubio et al. (2018). *Addressing security in OCPP*. NICS Lab – UMA