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

1. Anomali Tanımı

OCPP (Open Charge Point Protocol), şarj istasyonları ile merkezi yönetim sistemleri arasında iki yönlü veri iletimini sağlayan bir haberleşme protokolüdür.
Protokol üzerinden; kullanıcı kimlik bilgileri, şarj seansı tanımlayıcıları (token, idTag), sayaç verileri gibi hassas bilgiler iletilmektedir.

Ancak TLS (Transport Layer Security) desteği olmayan ya da yanlış yapılandırılmış sistemlerde bu veriler açık şekilde taşınır.
Ağ dinlemesi (sniffing) gibi basit yöntemlerle bu bilgiler **ele geçirilebilir**, taklit edilebilir veya kötüye kullanılabilir.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama
Protokol	Şifreleme zorunluluğu olmaması	OCPP 1.6 ve öncesi sürümlerde TLS opsiyoneldir.
Yapılandırma	Yanlış veya eksik TLS uygulaması	Sertifikaların eksikliği veya istemci doğrulamasının devre dışı bırakılması.
Uygulama	Kimlik bilgilerinin açık metin taşınması	SessionId, idTag gibi öğelerin mesajlarda açık şekilde iletilmesi.
Kategori	**Olası Sebep**	**Açıklama**

3. Olası Riskler ve Etkiler

- Kullanıcı kimlik bilgilerinin üçüncü kişiler tarafından izinsiz ele geçirilmesi
- Oturum tokenlarının çalınarak şarj işlemlerinin taklit edilmesi
- Sayaç verilerinin manipülasyonu ile faturalama süreçlerinin bozulması
- GDPR veya KVKK gibi veri koruma yasalarına aykırılık ve yasal yaptırımlar
- Kullanıcıların güven kaybı ve hizmet sağlayıcının itibarı üzerinde olumsuz etki

4. İlgili Standart / Referans

- **OCPP 1.6 / 2.0.1 Specification** – Open Charge Alliance
- **ISO 15118-2** – Vehicle to Grid Communication Interface

- **OWASP A3 & A6** – Sensitive Data Exposure / Security Misconfiguration
- **IEC 62443** – Industrial Communication Network Security
- **GDPR / KVKK** – Kişisel Verilerin Korunması Mevzuatı

5. Çözüm Önerileri (kolay uygulanabilir, maddeler halinde)

Yazılım Düzeyinde:

Ağ Katmanında:

- OCPP haberleşmesinde TLS 1.2 veya üstü protokoller zorunlu hale getirilmelidir
- Sertifika zinciri güvenilir bir otoriteden alınmalı ve düzenli olarak güncellenmelidir

Uygulama Katmanında:

- Kimlik bilgileri, token ve sayaç verileri gibi öğeler şifreli olarak taşınmalıdır
- OCPP mesaj formatı içinde, hassas verilerin masking veya hashlenmiş biçimde kullanılması önerilmelidir

Denetim ve Test:

- Penetrasyon testlerinde sniffing ve replay saldırılarına karşı direnç test edilmelidir
- Geliştirilen sistemlerde "secure-by-default" prensibi uygulanmalıdır

6. Sonuç ve Değerlendirme

OCPP üzerinden taşınan kimlik, token ve sayaç verilerinin şifrelenmemesi; hem kullanıcı gizliliğini hem de sistem güvenliğini doğrudan tehdit eder.
Basit ağ dinleme teknikleriyle bu veriler ele geçirilebilir ve saldırganlar tarafından suistimal edilebilir.

Bu nedenle, veri gizliliği odaklı bu açıklık **yüksek öncelikli** olarak değerlendirilmelidir ve gerek protokol düzeyinde gerekse uygulama düzeyinde gerekli önlemler mutlaka alınmalıdır.

.

7. Kaynaklar

- Open Charge Alliance. (2020). *OCPP 2.0.1 Specification*. [https://www.openchargealliance.org/]
- ISO 15118-2 – *Vehicle-to-Grid Communication Interface*
- OWASP Foundation – *Top 10 Web Application Security Risks*
- M. Stelios et al. (2023). *Survey on OCPP Security Issues*. arXiv:2207.01950

- IEC 62443 – *Industrial Automation and Control Systems Security*