BELGE BAŞLIĞI: AÇIK ŞARJ NOKTASI PROTOKOLÜ (OCPP) SÜRÜMLERİNDE İLETİŞİM GÜVENLİĞİ VE KİMLİK DOĞRULAMA ANALİZİ

BELGE TARİHİ: 2 KASIM 2025

1. Amaç

Bu doküman, Açık Şarj Noktası Protokolü (OCPP) sürümleri olan 1.6J, 2.0.1 ve 2.1 arasındaki temel güvenlik farklarını, özellikle iletişim kanalı güvenliği (Man-in-the-Middle saldırılarına karşı koruma) ve kimlik doğrulama mekanizmaları açısından analiz etmek amacıyla hazırlanmıştır. Bu analiz, mevcut ve gelecekteki elektrikli araç şarj altyapılarının güvenlik duruşunu değerlendirmek için teknik bir temel sağlamaktadır.

2. Kapsam

Bu analiz, Şarj İstasyonu (Charge Station - CS) ile Merkezi Yönetim Sistemi (Charging Station Management System - CSMS) arasındaki OCPP iletişimini kapsamaktadır. İki ana sürüm ailesi incelenmiştir:

- OCPP 1.6J (Güvenlik Eklentisi ile)
- OCPP 2.0.1 ve 2.1 (Entegre Güvenlik Modeli ile)

3. OCPP 1.6J Güvenlik Modeli

3.1. Protokol Durumu

OCPP 1.6J, mevcut durumda sahadaki kurulumlarda en yaygın olarak kullanılan protokoldür.

3.2. Güvenlik Yaklaşımı

Güvenlik özellikleri, OCPP 1.6J'nin çekirdek spesifikasyon belgesine dahil edilmemiştir. İletişim güvenliği, Open Charge Alliance (OCA) tarafından yayınlanan **"OCPP 1.6 Edition 2 Security Whitepaper"** (Güvenlik Beyaz Kitabı)

başlıklı ayrı bir tavsiye dokümanı ile ele alınmıştır.

3.3. Güvenlik Beyaz Kitabı Tavsiyeleri

Bu ayrı doküman, protokolü güvenli hale getirmek için iki ana mekanizma önerir:

- **İletişim Şifrelemesi:** Şifresiz WebSocket (ws://) yerine, Taşıma Katmanı Güvenliği (TLS) sağlayan Güvenli WebSocket (wss://) kullanılmasını *şiddetle tavsiye eder*. Bu, iletişimin gizliliğini ve bütünlüğünü sağlayarak araya girme (Man-in-the-Middle) saldırılarına karşı koruma sağlar.
- **Cihaz Kimlik Doğrulaması:** İstasyonun CSMS'e kimliğini kanıtlaması için wss:// bağlantısı kurulurken HTTP Temel Kimlik Doğrulama (HTTP Basic Authentication) kullanılmasını tavsiye eder.

3.4. Tespit Edilen Zafiyet Kaynağı

Bu güvenlik önlemlerinin ana protokolde "zorunlu" yerine, ayrı bir dokümanda "tavsiye" olarak belirtilmesi, birçok üreticinin ve operatörün bu özellikleri uygulamamasına yol açmıştır. Bu nedenle, birçok üretici 1.6'yı kurarken wss:// (Güvenli WebSocket) veya mTLS gibi güvenlik önlemlerini **uygulamamıştır**. Sonuç olarak, sahadaki çok sayıda OCPP 1.6J tabanlı sistem, şifresiz ws:// üzerinden iletişim kurmakta ve bu durum, araya girme, veri manipülasyonu ve oturum çalma saldırılarına karşı tamamen savunmasız olmalarına neden olmaktadır.

4. OCPP 2.0.1 ve OCPP 2.1 Güvenlik Modeli

4.1. Protokol Durumu

OCPP 2.0.1 ve en güncel sürüm olan 2.1, güvenliği "sonradan eklenen" bir özellik olarak değil, protokolün "çekirdek" bir bileşeni olarak ele alan modern standartlardır.

4.2. Güvenlik Yaklaşımı

OCPP 2.0.1 ve 2.1, güvenliği "Güvenlik Profilleri" (Security Profiles) adı verilen standartlaştırılmış bir yapı içinde zorunlu hale getirir. Bu profiller, bir cihazın veya sistemin protokole uyumlu sayılabilmesi için desteklemesi gereken minimum

güvenlik seviyelerini net bir şekilde tanımlar.

En Güncel Sürüm: OCPP 2.1

- Bu sürüm, Open Charge Alliance (OCA) tarafından yayınlanan en yeni versiyondur.
- **OCPP 2.0.1**'in üzerine inşa edilmiş bir iyileştirme sürümüdür. 2.0.1'deki bazı belirsizlikleri giderir, küçük hataları düzeltir ve ek fonksiyonlar (özellikle şebeke etkileşimi ve büyük ölçekli istasyon yönetimi için) getirir.

Modern Standart: OCPP 2.0.1

- Bu, asıl **büyük devrim niteliğindeki** sürümdür.
- Sizin güvenlik araştırmanız için en kritik özellikler bu sürümle birlikte standart hale gelmiştir:
- **Gelişmiş Cihaz Yönetimi**
- **ISO 15118 Desteği** (Araçla doğrudan iletişim - V2G/Vehicle-to-Grid)
- **Yerleşik Güvenlik (Security by Design):** Güvenli firmware güncellemeleri, TLS (şifreli iletişim) ve istemci (istasyon) sertifikaları (mTLS) için net profiller (Security Profile 1, 2, 3) tanımlar.

4.3. Güvenlik Profilleri Tanımları

Security Profile 1 (Güvenlik Profili 1):

- Açıklama: Herhangi bir güvenlik önlemi içermez. İletişim şifresiz (ws://) olarak gerçekleşir.
- Kullanım: Spesifikasyonda, bu profilin yalnızca fiziksel olarak tamamen güvenli ve izole edilmiş ağlarda (örn. kapalı laboratuvar ortamları) veya başka bir yöntemle (örn. donanımsal VPN) şifrelenmiş ağlarda test amacıyla kullanılabileceği, internet üzerinden kullanımının kesinlikle uygun olmadığı belirtilir.

Security Profile 2 (Güvenlik Profili 2):

- Açıklama: TLS ile sunucu taraflı kimlik doğrulaması.
- Gereklilik: wss:// kullanımını **zorunlu** kılar. İstasyon (istemci), bağlandığı CSMS'in (sunucu) sertifikasını doğrulamak zorundadır.
- Sağladığı Koruma: İletişimi şifreleyerek Man-in-the-Middle (MitM)

saldırılarını ve veri manipülasyonunu engeller.

Security Profile 3 (Güvenlik Profili 3):

- Açıklama: Karşılıklı TLS (mTLS) ile kimlik doğrulama.
- Gereklilik: Güvenlik Profili 2'ye ek olarak, istasyonun da CSMS'e bir istemci sertifikası (client-side certificate) sunarak kendi kimliğini kriptografik olarak kanıtlamasını **zorunlu** kılar.
- Sağladığı Koruma: MitM saldırılarına ek olarak, "istasyon taklidi" (device spoofing) saldırılarını da engeller.

4.4. Zorunluluk ve Uyumluluk

OCPP 2.0.1 ve 2.1 spesifikasyonlarına göre, bir CSMS veya istasyonun "OCPP 2.0.1/2.1 Uyumlu" olarak sertifikalandırılabilmesi için en az Güvenlik Profili 2'yi desteklemesi zorunludur . Güvenlik Profili 3 ise en yüksek güvenlik seviyesi olarak *şiddetle tavsiye edilir* .

5. Sonuç

OCPP 1.6J ile OCPP 2.x sürümleri arasındaki güvenlik farkı temel bir mimari farkıdır.

- **OCPP 1.6J:** Güvenliği *opsiyonel* bir eklenti olarak ele alır. Bu durum, yaygın uygulamalarda ciddi güvenlik zafiyetlerine yol açmıştır.
-
- **OCPP 2.0.1 / 2.1:** Güvenliği *zorunlu* ve *entegre* bir bileşen olarak tanımlar. Güvenlik Profili 2'nin zorunlu kılınması, Man-in-the-Middle saldırılarına karşı temel bir korumayı garanti altına alır.

Sonuç olarak, yeni altyapı projelerinde OCPP 2.0.1 veya üzeri sürümlerin tercih edilmesi ve en az Güvenlik Profili 2 (Güvenlik Profili 3'ün hedeflenmesi) ile yapılandırılması, şarj altyapısının siber güvenliği için kritik bir gerekliliktir. Mevcut OCPP 1.6J sistemleri için ise "Security Whitepaper" dokümanındaki tavsiyelerin (özellikle wss:// kullanımı) ivedilikle uygulanıp uygulanmadığı denetlenmelidir.

Sacide Aişenur Direk