Açık Şarj Noktası Protokolü (OCPP) Temelli Elektrikli Araç Şarj Altyapısı İçin Kapsamlı Siber Güvenlik Risk Değerlendirmesi (SWOT ANALİZİ)

I. EV Şarj Ağlarında Protokol Güvenlik Açıklarına Giriş

I. A. EV Altyapısında OCPP'nin Kritik Rolü ve Birlikte Çalışabilirlik

Elektrikli araç (EV) şarj altyapısının yaygınlaşması, şarj noktaları (CP) ile merkezi yönetim sistemleri (CSMS) arasındaki iletişimi sağlayan temel protokol olan Açık Şarj Noktası Protokolü'nü (OCPP) kritik bir hale getirmiştir.[1] OCPP, farklı donanım ve yazılım sağlayıcıları arasında kesintisiz iletişimi mümkün kılarak tedarikçi kilitlenmesini (vendor lock-in) önler ve böylece ölçeklenebilir bir EV altyapısının temelini oluşturur.[3] Protokolün bu rolü, hem EV şarj deneyiminin sorunsuz olmasını hem de sağlayıcılar için sürdürülebilir, birlikte çalışabilir bir ağın varlığını güvence altına almaktadır.[4]

Şu anda pazarda baskın olarak kullanılan üç ana OCPP sürümü bulunmaktadır: 2015 yılında piyasaya sürülen ve hala yaygın olarak kullanılan OCPP 1.6; 2020'de yayımlanan OCPP 2.0.1; ve 2025'te yayımlanan en yeni standart olan OCPP 2.1.[3] Bu versiyonlar arasındaki farklar, yalnızca işlevsellik değil, aynı zamanda kritik güvenlik tanımlamaları açısından da büyük önem taşımaktadır.[1] OCPP 2.0.1'in 2024 yılında IEC 63584: 2024 uluslararası standardı olarak onaylanması, gelecekteki EV altyapısı için zorunlu güvenlik ve uyumluluk seviyesini belirlemiştir.[3]

I. B. Eski Protokol Dağıtımlarındaki Güvenlik Açığı Borcu (OCPP 1.6 Odaklı)

Elektrikli araç şarj istasyonları, modern kentleşmenin kritik altyapı bileşenleri olarak kabul edilmektedir. Bu istasyonların siber güvenlik zaafiyetleri, sadece veri hırsızlığı değil, aynı zamanda önemli siber-fiziksel riskler ve gizlilik sorunları da doğurmaktadır.[1] OCPP 1.6, modern EV şarj

ağlarının temelini atmış olsa da, güvenlik tanımlamalarındaki doğal sınırlamalardan muzdariptir. Bu durum, operatörlerin genellikle protokolün kendi gücü yerine isteğe bağlı ve harici güvenlik önlemlerine güvenmesini gerektirir.[2] Bu durum, yaygın olarak kullanılan OCPP 1.6'nın mevcut ve yeni, daha güvenli standartlarla (2.0.1 ve 2.1) karşılaştırıldığında önemli bir düzenleyici yükümlülük boşluğu oluşturduğu anlamına gelir.

Bu protokolün yaygınlığı göz önüne alındığında, operatörler zorunlu güvenlik önlemlerini uygulamadığı veya protokolü modernize etmediği sürece ciddi bir "güvenlik açığı borcu" biriktirmektedir. Tek bir şarj noktasındaki güvenlik ihlali, bütün bir şarj ağına ve dolayısıyla daha geniş enerji şebekesine yayılabilir, bu da sorunun basit bir bilgi teknolojisi (IT) güvenlik açığından ulusal kritik altyapı arıza noktasına yükselmesine neden olur. Öte yandan, OCPP 2.0.1'in uluslararası IEC standardı olarak kabul edilmesi [3], 1.6 tabanlı ve sertifikasız uygulamaların sigorta sağlayıcıları ve gelecekteki yasal denetimler karşısında baskı altına gireceğini gösterir.[4] Bu, operatörler için proaktif güvenlik tedbirlerini hızlandırma ihtiyacını daha da pekiştirmektedir.

I. C. EV Besleme Ekipmanlarındaki (EVSE) Siber-Fiziksel Risklerin (S-F R) Genel Görünümü

Siber saldırıların risk profili, yalnızca finansal verilerin ele geçirilmesinden öteye geçerek, fiziksel altyapının kontrolünü hedef almaktadır. EV şarj altyapısının tehlikeye atılması, yetkisiz enerji tüketimine, hizmet reddi (DoS) saldırıları yoluyla ulaşım ağlarının kesintiye uğramasına veya şebeke talebinin manipülasyonuna neden olabilir. En kritik risklerden biri, şarj istasyonlarının etkilenen kurulumlarında ağa bitişik saldırganların rastgele kod çalıştırmasına (RCE) olanak tanıyan güvenlik açıklarıdır. Bu tür bir açık (örneğin, CVE-2024-23971) kök (root) bağlamında kod yürütülmesine izin verebilir.[6] Kullanıcı tarafından sağlanan dizenin sistem çağrısı için kullanılmadan önce uygun şekilde doğrulanmamasından kaynaklanan bu tür mantık kusurları, tam sistem ele geçirilmesine ve kalıcı kötü amaçlı yazılım kurulumuna yol açabilecek en yüksek önem düzeyine sahip siber-fiziksel tehditleri temsil etmektedir.

II. OCPP 1.6 Temel Güvenlik Analizi ve İletişim Boşlukları

II. A. Mimari İncelemesi: Şarj Noktası (CP) ile Merkezi Sistem Yönetim Hizmeti (CSMS) Arasındaki İletişim

OCPP 1.6'da CP ile CSMS arasındaki bağlantı için temel iletişim standardı OCPP-J, yani WebSocket

üzerinden JSON kullanımıdır.[7] Protokol işlevselliği, farklı profillerde gruplandırılmış mesajlara dayanır. Uygulaması zorunlu olan Temel (Core) profil, BootNotification ve Authorize.req gibi kritik operasyonel akışları içerir.[7]

Authorize.req mesaj dizisi, sistemin kalbinde yer alır. Elektrikli araç sahibi şarjı başlatmadan veya durdurmadan önce, Şarj Noktası işlemi yetkilendirmek zorundadır. Şarj Noktası, enerjiyi yalnızca yetkilendirme başarılı olduktan sonra sağlamalıdır.[7] Bu katı operasyonel gereklilik, yetkisiz şarj elde etmeye çalışan saldırganlar için yetkilendirme sürecini birincil hedef haline getirmektedir. Bu nedenle, ortadaki adam (MitM) saldırısı veya kimlik sahtekarlığı yoluyla yetkilendirme mesajının manipüle edilmesi, doğrudan finansal kayıp riskine yol açmaktadır.

II. B. OCPP 1.6'da TLS 1.2 Üzerinden WebSocket Kullanımının Zayıflıkları

OCPP 1.6 standardı, güvenli bağlantı için WebSocket üzerinden TLS kullanımını tavsiye etse de [4], bu uygulamanın doğasında bulunan ve deneysel olarak kanıtlanmış güvenlik açıkları mevcuttur. Yapılan analizler, TLS 1.2 kullanılsa bile, oturum açığa çıkarılması ve potansiyel sömürü için kritik önem taşıyan bilgilerin şifresi çözülmüş paketlerde açık metin olarak kaldığını göstermiştir.[9]

Bu kritik veriler arasında kullanılan şifre paketleri (cipher suites), oturum kimliği (session ID), sunucu adresi ve uygulama protokolleri bulunmaktadır.[9] Bu verilerin açıkta olması, saldırganlara sofistike bir Ortadaki Adam saldırısı başlatmak için gereken ilk ayak izini sağlar. Güvenlik açığı, şifreleme eksikliğinden ziyade, şarj noktası (CP) veya merkezi sistem (CSMS) uygulamasının TLS 1.2 oturum kurma ve el sıkışma aşamalarını hatalı ele almasından kaynaklanmaktadır. Bu durum, modern TLS sürümlerine geçişi veya kritik alanlar için uygulama katmanı şifrelemesini zorunlu kılmayı kaçınılmaz kılmaktadır. Ayrıca, OCPP 1.6'nın güvenli olmayan dağıtımlarda şifrelenmemiş WebSocket iletişimine güvenme potansiyeli de bulunmaktadır, bu da MitM saldırılarını doğrudan kolaylaştırır.[8]

II. C. OCPP 1.6 Profillerindeki Sınırlı Kimlik Doğrulama Mekanizmaları

OCPP 1.6'nın modüler yapısı, temel işlevselliği (Core profili) zorunlu tutarken, aygıt yazılımı yönetimi, yerel yetkilendirme listesi yönetimi ve rezervasyonlar gibi güvenlik açısından kritik özellikleri isteğe bağlı profillerde gruplar.[7] Bu isteğe bağlılık, ağ güvenliğinin, bir satıcının veya operatörün seçtiği en zayıf isteğe bağlı uygulamaya bağlı olması anlamına gelir. Bu nedenle, operatörler protokolün doğasından gelen güce güvenmek yerine, sürekli olarak güvenlik açıklarını yamalamak zorunda kalır, bu da karmaşıklığı ve insan hatası potansiyelini artırır.

Şarj için kimlik doğrulama genellikle bir tanımlayıcıya (RFID etiketi veya mobil uygulama kimliği) dayanır. Protokol, enerji arzına başlamadan önce CP'nin bir Authorize.req göndermesini gerektirse de [7], bu kimlik tabanlı basit yetkilendirme modeli, kimlik sahtekarlığı saldırıları için kritik bir güvenlik açığı yüzeyi oluşturmaktadır.