Açık Şarj Noktası Protokolü (OCPP) Temelli Elektrikli Araç Şarj Altyapısı İçin Kapsamlı Siber Güvenlik Risk Azaltma Senaryosu

III. Detaylı Tehdit Modellemesi: OCPP 1.6'ya Yönelik Aktif Saldırı Vektörleri

III. A. İletişim Önleme ve Ortadaki Adam (MitM) Saldırıları

OCPP 1.6 ortamlarında MitM saldırıları, genellikle Adres Çözümleme Protokolü (ARP) sahtekarlığı veya önbellek zehirlenmesi ile başlar. Saldırgan, CP ile CSMS arasındaki trafiği yakalamak ve değiştirmek için kendi MAC adresini hedef IP adresiyle ilişkilendirir.[8] Bu yöntem, saldırganın istemci ve sunucu arasına görünmez bir şekilde oturmasını sağlar.

Bu tür bir müdahale, TLS kullanılmıyorsa açık metin iletişimin izlenmesine veya daha karmaşık MitM saldırılarında, Bölüm II'de belirtildiği gibi, şifreli olsa bile açığa çıkan oturum meta verilerinin sömürülmesine olanak tanır.[9] Sonuç olarak, saldırgan oturumları ele geçirebilir, yanlış komutları (örneğin, StartTransaction.req) enjekte edebilir veya mevcut veri akışlarını değiştirebilir. Bu oturum manipülasyonu, yetkisiz şarj işlemleri başlatmanın ve hizmetleri kesintiye uğratmanın temel yoludur.

III. B. Kimlik Sahtekarlığı ve Temsil Saldırıları

Kimlik sahtekarlığı saldırıları, OCPP 1.6 ortamlarındaki zayıf yetkilendirme mekanizmalarını doğrudan hedefler.[5]

1. **Şarj Noktası Temsili (Impersonation):** Kötü niyetli bir aktör, meşru bir Elektrikli Araç

Şarj İstasyonunun (EVCS) benzersiz kimliğini (ID) kullanarak kendisini o CP gibi gösterebilir.[5] Bu saldırının amacı, yanlış durum güncellemeleri rapor etmek, yetkisiz işlemleri başlatmak veya sahte BootNotification mesajlarıyla CSMS arka ucunu aşırı yükleyerek Hizmet Reddi (DoS) oluşturmaktır.

2. **Kullanıcı Kimliği Sahtekarlığı:** Saldırgan, başka bir meşru kullanıcının ID'sini kullanarak yetkisiz şarj işlemleri başlatır.[5] Bu, genellikle Authorize.req mesaj akışını çevreleyen mantığı hedefleyerek, yetkisiz enerji tüketimine ve yanlış faturalandırma kayıtlarına yol açar. Yetkilendirme katmanını atlayan veya manipüle eden herhangi bir saldırı (MitM, kimlik sahtekarlığı veya mantık hatası), anında ve yetkisiz finansal kayba neden olur.[7]

III. C. Protokol Mantığı ve Uygulama Kusurlarının Sömürülmesi

Saldırılar, sadece iletişimi değil, şarj sürecinin mantıksal durum makinesini de hedef alabilir (örneğin, yetkisiz bir ID ile bir işlemi durdurmaya çalışmak veya zorla durum değişikliği yapmak).

Bu alandaki en büyük tehdit, uygulamaya özgü güvenlik açıklarından kaynaklanmaktadır. Örneğin, CVE-2024-23971 güvenlik açığı, OCPP mesajlarının işlenmesindeki bir kusuru ortaya koymaktadır. Bu kusur, kullanıcı tarafından sağlanan bir dizenin sistem çağrısını yürütmek için kullanılmadan önce uygun şekilde doğrulanmamasından kaynaklanır.[6] Bu tür bir mantık kusuru, ağa bitişik saldırganların, kimlik doğrulamasına gerek kalmadan etkilenen şarj istasyonlarında kök (root) bağlamında rastgele kod çalıştırmasına olanak tanır.[6] Bu durum, en yüksek öneme sahip siber-fiziksel tehdit sınıfına aittir, çünkü sistemin tamamen ele geçirilmesine, fiziksel altyapıya potansiyel hasar verilmesine veya EV ağının güvenilir içinden dağıtılmış, sistemik saldırılar başlatmak için bir köprü noktası olarak kullanılmasına olanak tanır.

Ağa bitişik RCE [6] ve Kimlik Temsili [5] tehditlerinin birleşimi, çok aşamalı bir saldırı stratejisine işaret eder: önce RCE yoluyla tek bir CP'de kök kabuk elde edilir ve ardından bu ele geçirilmiş CP, istasyonun yükseltilmiş ağ ayrıcalıklarını kullanarak CSMS arka ucuna karşı yüksek hacimli kimlik sahtekarlığı ve hizmet reddi saldırıları başlatmak için kullanılır.

Aşağıdaki tablo, OCPP 1.6'ya yönelik tespit edilen ana saldırı vektörlerini ve bunların potansiyel etkilerini özetlemektedir:

Table 1: Summary of Identified OCPP Cyberattack Vectors and Impact (Tespit Edilen OCPP Siber Saldırı Vektörlerinin ve Etkilerinin Özeti)

Saldırı Vektörü	Etkilenen OCPP Sürümü	Mekanizma/Sömürülen Güvenlik Açığı	Risk Katmanı	Potansiyel Sonuç	Kaynak
Ortadaki Adam (MitM)	1.6 (TLS 1.2 ile bile)	ARP Sahtekarlığı; Güvenli olmayan oturum meta verilerinin (şifre paketleri, oturum kimliği) önlenmesi [9, 8]	İletişim (L4/L7)	Oturum Ele Geçirme, yetkisiz komut değiştirme, veri sızdırma.	[9, 8]
Şarj Noktası/Kullanıcı Kimliği Sahtekarlığı	1.6	İşlemleri başlatmak için meşru benzersiz kimliklerin veya kullanıcı kimlik bilgilerinin yetkisiz kullanımı [5]	Uygulama/ Mantık (L7)	Yetkisiz enerji kullanımı (finansal kayıp), yanlış raporlama yoluyla DoS.	[5]
Uzaktan Kod Çalıştırma (RCE)	1.6 (Uygulama Bağımlı)	OCPP mesajlarında kullanıcı tarafından sağlanan dizelerin uygun	Uygulama/İşletim Sistemi (L7/L3)	Sistem ele geçirme (kök bağlamında), fiziksel altyapı hasarı,	[6]

		şekilde doğrulanmaması (örneğin, CVE-2024-23971) [6]		ağda pivot noktası oluşturma.	
Taşkın/Yanlış Veri Enjeksiyonu (YVE)	1.6	İletişim kanalının aşırı yüklenmesi veya yanıltıcı işlem verilerinin enjekte edilmesi [5]	Uygulama/İletişim	Hizmet kesintisi, yanlış enerji raporlaması, finansal manipülasyon.	[5]

IV. Protokol Modernizasyonu Yoluyla Stratejik Azaltım (OCPP 2.0.1/2.1)

IV. A. OCPP 2.0.1 (IEC 63584: 2024) Kabulünün Güvenlik Zorunluluğu

OCPP 2.0.1'in IEC 63584: 2024 uluslararası standardı olarak onaylanması, protokol modernizasyonunu bir seçenekten zorunluluğa dönüştürmüştür.[1] OCPP 2.0, temel olarak güvenlik, ölçeklenebilirlik ve gelişmiş enerji yönetimine odaklanarak 1.6'dan önemli bir ilerleme kaydetmiştir.[2]

OCPP 2.0, Elektrikli Araç Besleme Ekipmanını (EVSE) mantıksal bir birim olarak tanımlayan hiyerarşik bir aygıt modeli sunar. Bu model, 1.6'daki basit bağlantı noktası tanımlamasının aksine, çoklu konektörlü istasyonlar gibi karmaşık yapılandırmaların daha iyi yönetilmesini sağlar.[2] Güvenlik açısından bu, güvenlik politikalarının ve erişim kontrollerinin yalnızca fiziksel bağlantı düzeyinde değil, EVSE düzeyinde mantıksal olarak uygulanabilmesi anlamına gelir.

IV. B. Resmi Güvenlik Profilleri ve Zorunlu Gereklilikler

OCPP 2.0.1/2.1, güvenliği isteğe bağlı bir katman olmaktan çıkarıp protokolün ayrılmaz bir parçası haline getirir. Bu yeni sürümler, aşamalı olarak daha güçlü koruma sağlayan üç açık güvenlik profilini tanımlar.[1]

Bu profillerden biri, **Güvenlik Profili 1 - Temel Kimlik Doğrulamasıyla Güvenli Olmayan**, herhangi bir şifreleme veya kimlik doğrulaması olmaksızın düz metin iletişimi içerir. Araştırmalar, bunun yalnızca sıkı kontrol edilen test ortamları için uygun olduğunu ve üretim ortamlarında, verilerin ele geçirilmesi ve yetkisiz manipülasyon riskleri nedeniyle önemli riskler taşıdığını vurgulamaktadır.[1] Bununla birlikte, bu profilin varlığını sürdürmesi, operatörlerin maliyeti güvenliğe tercih etmesi durumunda hala güvensiz dağıtımlara izin verme riski taşımaktadır.

Daha yüksek profiller, zorunlu istemci tarafı sertifikaları, uçtan uca şifreleme ve güçlü kriptografik önlemler gibi katı gereklilikleri tanımlar. OCPP 1.6'nın güvenliği isteğe bağlı bir katman olarak ele almasına karşın, 2.0.1/2.1'in güvenliği resmi profiller ve açık işlevler aracılığıyla zorunlu bir yetenek haline getirmesi, satıcılar ve operatörler için güvenlik taban gereksinimini önemli ölçüde yükseltmektedir.

IV. C. Gelişmiş Kimlik Doğrulama ve Sertifika Yönetimi

OCPP 2.0.1/2.1, 1.6'da kullanılan basit ID etiketi yetkilendirmesine olan bağımlılıktan uzaklaşarak, zorunlu sertifika tabanlı kimlik doğrulamaya geçer. Bu, kimlik sahtekarlığı ve MitM saldırılarının engellenmesi için kritik bir adımdır.

Yeni protokol, kriptografik materyalin yönetimi için açık mesajlar sağlar: InstallCertificate, DeleteCertificate ve GetInstalledCertificateIds.[10] Bu özel işlevsellik, CSMS'nin güven zincirini uzaktan ve güvenli bir şekilde yönetmesine olanak tanır, bu da hızlı sertifika rotasyonu ve iptali sağlar. Bu sayede, bir saldırganın yalnızca bir ID'yi taklit etmesi yerine, meşru bir CP'nin özel anahtarını tehlikeye atması gerektiği için, Şarj Noktası Temsili riskini önemli ölçüde azaltır.[5]

IV. D. Gelecek Güvenlik Standartları ve V2X Desteği

OCPP 2.1, Plug & Charge ve gelişmiş çift yönlü güç transferi (V2X) için temel teşkil eden ISO 15118-20 desteğini açıkça tanıtmaktadır.[3] Bu entegrasyon, güvenliği ve kimlik doğrulamayı aracın kimliği ve şarj oturumuyla doğal olarak ilişkilendirerek, basit RFID etiketlerinden daha yüksek bir güvence katmanı sunar.

Ayrıca, 2.0.1/2.1'deki gelişmiş akıllı şarj yetenekleri, şebeke koşullarına veya enerji fiyatlarına göre dinamik, gerçek zamanlı profil güncellemelerine izin verir.[2] Bu dinamik enerji dağıtımının manipüle edilmesini önlemek ve şebeke istikrarını korumak için sağlam güvenlik mekanizmalarının varlığı zorunludur.

OCPP 1.6 ve 2.0.1/2.1 arasındaki temel güvenlik farklılıkları, aşağıdaki tabloda özetlenmiştir:

Table 2: Key Security Feature Comparison: OCPP 1.6 vs. 2.0.1/2.1 (Temel Güvenlik Özellikleri Karşılaştırması: OCPP 1.6 ve 2.0.1/2.1)

Güvenlik Özelliği	**OCPP 1.6**	**OCPP 2.0.1 / 2.1**	**Güvenlik Etkisi**	**Kaynak**
Protokol Temeli	Bağlantı ve temel ölçüm odaklı.	Güvenlik, akıllı şarj ve V2X (2.1) odaklı.	Stratejik risk azaltma ve geleceğe yönelik hazırlık.	[2, 3]
Güvenlik Profilleri	Örtük; isteğe bağlı TLS'ye güven; standartlaştırılmış seviye yok.	Zorunlu şifreleme/kimlik doğrulamayı tanımlayan resmi üç katmanlı profiller (1, 2, 3).[1]	Zorunlu bir güvenlik taban çizgisi oluşturur.	[1]
Kimlik Doğrulama	Öncelikle ID etiketi yetkilendirmesi; temel TLS	Zorunlu sertifika tabanlı kimlik doğrulama; ISO 15118-20	Kimlik sahtekarlığı ve MitM saldırılarını	[7, 3]

	desteği (isteğe bağlı).	entegrasyonu desteği.[3]	önemli ölçüde azaltır.	
Sertifika Yönetimi	Temel/Sınırlı (özel yöntemler veya manuel müdahale gerektirir).[10]	Açık işlevler: InstallCertificate, DeleteCertificate, GetInstalledCertificateIds.	Dinamik, merkezi PKI yönetimi sağlar.	[10]
Aygıt Modeli	Basit bağlantı noktası seviyesinde tanımlama.[2]	Mantıksal yönetim için hiyerarşik EVSE yapısı.[2]	Politika uygulamasını ve güvenlik denetim kapsamını iyileştirir.	[2]

V. Gelişmiş Saldırı Tespiti ve Adaptif Savunmalar

V. A. EV Altyapısında Geleneksel Güvenlik Yöntemlerinin Sınırlamaları

Geleneksel ağ güvenliği çözümleri (güvenlik duvarları, genel saldırı tespit sistemleri) genellikle geçerli OCPP mesaj yapılarını manipüle eden veya durum makinesi mantığını sömüren uygulama katmanı saldırılarını (örneğin, Yanlış Veri Enjeksiyonu - YVE, Temsil [5]) tespit etmede yetersiz kalır. Etkili savunma, paket yakalama seviyesinin ötesine geçmelidir.

Özellikle dikkate alınması gereken bir tehdit, saldırganların yapay zeka (AI) modellerinden kaçınmak için düşmanca AI tekniklerini kullanabilmesidir. Bu durumda, saldırılar ağ paketlerini yakalamaktan kaçınabilir ve tespit edilemez kalabilir.[5] Bu tür senaryolarda, saldırıların tespiti sistemin operasyonel durumunu, yani potansiyel bir saldırının belirtilerini gözlemlemeye kaydırılmalıdır.

V. B. Ağ Trafiği Analizi için Federasyonel Öğrenme (FL) Uygulaması

EV şarj istasyonlarının büyük ölçekli ve dağıtık doğası, Federasyonel Öğrenme (FL) tabanlı bir Saldırı Tespit Sistemi (IDS) mimarisini ideal bir çözüm olarak konumlandırmaktadır.[5] FL, birden fazla Kaynaklar Arası Nesnelerin İnterneti (IoT) verisini kullanarak gelişmiş saldırı tespit sonuçları elde etmeye olanak tanır, bunu yaparken de özel bilgilerin gizliliğini korur.[5]

FL mimarisinde, istemciler birden çok EV şarj merkezinde konumlandırılır ve bu istemciler yerel OCPP 1.6 ağ trafiğini analiz eder.[5] İstemciler, ham verileri paylaşmak yerine, yerel olarak eğitilmiş modellerin ağırlıklarını küresel bir AI modelinin eğitimine katkıda bulunur. Bu, merkezi yaklaşımla neredeyse aynı performansı elde ederken, aynı zamanda gizliliği doğal olarak güvence altına alır.[5]

FL'nin etkinliği, FedProx, FedAvg ve FedTree gibi toplama yöntemlerinin, özellikle Yanlış Pozitif Oranı (FPR) ve F1 puanı açısından daha iyi sonuçlar verdiğini gösteren deneylerle desteklenmektedir.[5] FL, paylaşılan tehdit istihbaratı ihtiyacı ile özel veri gizliliği zorunluluğu arasındaki temel çatışmayı çözerek, siber güvenliği tescilli bir savunma probleminden ortak, endüstri çapında bir faydaya dönüştürür.

V. C. Özel Araçlar Kullanılarak Akış Tabanlı Saldırı Tespiti

OCPP 1.6 siber saldırılarını tespit etmek, protokolün özelliklerine odaklanan özelleşmiş akış istatistikleri gerektirir. Bu amaçla tasarlanan OCPPFlowMeter gibi araçlar kritik öneme sahiptir.[5] Bu araç, yalnızca ağ ve iletim katmanlarını değil, aynı zamanda OCPP 1.6 uygulama katmanını da kapsayan saldırıların tespitini sağlayan özellikler üretir.[5] OCPPFlowMeter, taşkın (flooding) saldırılarının yanı sıra, özellikle finansal manipülasyonu hedefleyen Yanlış Veri Enjeksiyonu (YVE) gibi uygulama katmanı saldırılarına karşı da etkililiğini göstermiştir.[5]

Ancak, bu tür gelişmiş savunma çözümlerinin uygulanması, her EV şarj merkezinin bir ana makineye ve port yansıtma özelliklerine sahip bir ağ anahtarına sahip olmasını gerektiren yüksek donanım ve kurulum gereksinimleri getirir.[5] Bu yüksek gereksinim, maliyet hassasiyeti olan tipik şarj istasyonu dağıtım modeliyle çelişir ve gelişmiş savunma seviyesinin şu anda yalnızca yüksek değerli, kritik merkezlerde uygulanabileceğini, daha küçük istasyonların ise savunmasız kaldığını gösterir.

Table 3: Key Feature Requirements for Application-Layer Flow Analysis (Uygulama Katmanı Akış Analizi İçin Temel Özellik Gereksinimleri)

Özellik Kategorisi	Gerekli Akış İstatistiği	Güvenlik Önemi/Tespit Edilen Saldırı	Kaynak
İşlem Durumu	Dakika başına başarısız Authorize.req denemesi sayısı.	Kaba kuvvet ID sahtekarlığı denemelerinin tespiti.[5]	[7, 5]
Bağlantı Bütünlüğü	WebSocket bağlantı sıfırlama/yeniden kurma isteklerinin sıklığı.	Aktif MitM girişimlerinin veya oturum kesintisinin göstergeleri.[9, 8]	[9, 5]
Mesaj Hacmi	Belirli çağrı türlerinin oranı (örn. StartTransaction, StopTransaction).	Taşkın veya Hizmet Reddi (DoS) saldırılarının tespiti.[5]	[5]
Veri Tutarlılığı	Enerji sayacı okumaları ile rapor edilen işlem durumu arasındaki korelasyon.	Faturalandırma manipülasyonunu hedefleyen Yanlış Veri Enjeksiyonu (YVE) tespiti.[5]	[5]
Sistem Komutları	Uzaktan komut kullanım oranı (örn. RemoteStartTransaction, GetLog).	Yetkisiz komut enjeksiyonunun veya tehlikeye girmiş yönetim erişiminin tespiti.	[10]

V. D. Gözlemsel Savunma Stratejileri

Saldırganlar paket yakalamadan kaçınmayı başarırsa, tespit stratejisi sistemin operasyonel belirtilerini gözlemlemeye odaklanmalıdır.[5] Bu, yetkisiz durum değişikliklerini, anormal enerji çekişini veya beklenmedik sistem yeniden başlatmalarını içerebilir.

Bu strateji, Şarj Noktasının Merkezi Sisteme SecurityEventNotification mesajları gönderme yeteneğinden yararlanmayı ve ayrıca GetLog komutuyla daha sonraki adli analizler için erişilebilecek güvenlik günlüklerini yerel olarak kaydetmeyi içerir.[10] Bu işlevsellik, saldırının belirtilerini aktif olarak bildirme ve kayıt altına alma imkanı sunarak, pasif ağ izlemeye bir tamamlayıcı görevi görür.

VI. Operasyonel Tavsiyeler ve Gelecek Güvenlik Yol Haritası

OCPP ortamlarında yüksek düzeyde güvenlik sağlamak, hem mevcut altyapının risklerini azaltmak hem de gelecekteki dağıtımların uluslararası standartlara uygun olmasını sağlamak için iki aşamalı bir strateji gerektirir.

VI. A. Mevcut OCPP 1.6 Dağıtımlarını Güvenli Hale Getirmek İçin Acil Adımlar

1. **Zorunlu TLS 1.3 Kullanımı:** TLS 1.2'deki oturum meta verilerinin açığa çıkması nedeniyle ortaya çıkan riskler göz önüne alındığında, hemen TLS 1.3'e geçiş yapılmalı ve TLS 1.2 kullanımı derhal yasaklanmalıdır.[9]
2. **Titizlikle Denetlenmiş Giriş Doğrulaması:** Protokol mantığı kusurlarını ve CVE-2024-23971 gibi RCE güvenlik açıklarını önlemek için, özellikle kullanıcı tarafından sağlanan verileri işleyen OCPP mesaj işleyicilerinde sıkı güvenlik kodu inceleme ve sanitasyon prosedürleri uygulanmalıdır.[6]
3. **Ağ Bölümleme (Segmentation):** ARP sahtekarlığı saldırılarını önlemek amacıyla, şarj istasyonlarının kendi yüksek düzeyde güvenli Sanal Yerel Alan Ağlarında (VLAN) izole edilmesi sağlanmalıdır.[8]

4. **Yerel Güvenlik Duvarı Uygulaması:** Güvenliği ihlal edilmiş aygıt yazılımı tarafından başlatılan sistem çağrılarını önlemek için katı çıkış filtrelemesi (egress filtering) uygulanarak harici iletişim kanalları sınırlandırılmalıdır.

VI. B. OCPP 2.0.1/2.1'e Aşamalı Geçiş Kılavuzu

1. **Yeni Dağıtımlarda Zorunluluk:** Tüm yeni EVSE dağıtımları, OCPP 2.0.1 veya 2.1 özelliklerine uymalı ve Güvenlik Profili 2 veya 3'ü uygulamalıdır; güvensiz Profil 1'den kesinlikle kaçınılmalıdır.[1]
2. **Emeklilik Çizelgesi:** Gelişmiş güvenlik özelliklerinden yoksun tüm OCPP 1.6 donanımları için kesin, kamuya açık bir emeklilik çizelgesi oluşturulmalıdır.
3. **CSMS Uyumluluğu:** Geçiş dönemi boyunca Merkezi Sistemin hem 1.6 hem de 2.x uç noktalarını yönetebilmesi sağlanmalı, 2.x'in açık sertifika yönetim mesajları kullanılarak merkezi sertifika yönetimine öncelik verilmelidir.[10] Bu, protokol modernizasyonu yoluyla kimlik temsilini azaltmak için hayati önem taşımaktadır.

VI. C. Zorunlu Güvenlik Konfigürasyonları

1. **Port Yansıtma ve Ana Makine Kurulumu:** Yüksek trafikli veya kritik şarj merkezleri için, gelişmiş FL tabanlı IDS çözümlerini çalıştırmak amacıyla gerekli donanıma (ana makine ve port yansıtma özellikli ağ anahtarı) yatırım yapılması zorunlu kılınmalıdır.[5]
2. **Gelişmiş Kayıt Tutma ve Olay Raporlama:** Etkili adli soruşturma ve belirti tabanlı tespiti sağlamak için güvenlik olaylarının kaydı ve uzaktan alınması (SecurityEventNotification ve GetLog aracılığıyla) zorunlu hale getirilmelidir.[10]

VI. D. Uzun Vadeli Strateji: V2X Güvenliği ve Şebeke Dayanıklılığının Entegrasyonu

Gelecek stratejisi, protokol modernizasyonunun sağladığı gelişmiş özelliklerin tam entegrasyonuna dayanmalıdır. OCPP 2.1'de tanıtılan Çift Yönlü Enerji Akışları (V2X) ve Dağıtılmış Enerji Kaynak (DER) Kontrolü için yeni işlevsel blokların entegrasyonu, ilgili ISO 15118-20 güvenlik zorunluluklarına sıkı sıkıya uyumu gerektirir.[3]

Son olarak, Adaptif Güvenlik Döngüsü oluşturulmalıdır. Bu döngüde, FL tabanlı IDS'den elde edilen saldırı tespit sonuçları, şarj profillerini ve yerel erişim kontrol listelerini doğrudan bilgilendirip güncelleyerek, ağın ortaya çıkan tehditlere karşı otonom olarak uyum sağlamasını ve dayanıklılığını artırmasını sağlar.

Sonuç

Kapsamlı analiz, yaygın olarak kullanılan OCPP 1.6 protokolünün iletişim (MitM), uygulama (Kimlik Sahtekarlığı) ve uygulama mantığı (RCE potansiyeli) katmanlarında önemli, sistemik güvenlik açığı borcu taşıdığını doğrulamaktadır. Bu zafiyetler, yetkisiz enerji tüketiminden ulusal şebeke güvenliğine kadar uzanan ciddi siber-fiziksel riskler yaratmaktadır.

Bu riskleri azaltmak için çift yönlü bir strateji zorunludur:

1. **Miras Sistemler İçin Telafi Edici Kontroller:** OCPP 1.6 dağıtımları için hemen TLS 1.3 zorunluluğu, titiz giriş doğrulaması ve ağ izolasyonu gibi katı ağ sertleştirme önlemleri uygulanmalıdır. Kritik merkezlerde, tescilli verilerin gizliliğini korurken tehdit istihbaratını paylaşarak uygulama katmanı saldırılarını tespit edebilen Federasyonel Öğrenme tabanlı Gelişmiş Saldırı Tespit Sistemlerine yatırım yapılmalıdır.
2. **Proaktif Protokol Modernizasyonu:** Operatörlerin, güvenliği zorunlu kılan resmi profiller, sertifika tabanlı kimlik doğrulama ve gelişmiş kriptografik yönetim yetenekleri sunan, yeni uluslararası standart olan OCPP 2.0.1 (IEC 63584: 2024) veya 2.1'e geçişi hızlandırması zorunludur. Bu modernizasyon, kimlik temsilini tasarımdan itibaren önleyerek ve V2X gibi geleceğin enerji gereksinimlerini güvenli bir şekilde destekleyerek uzun vadeli dayanıklılık sağlar.

Güvenlik riski, tekil bir istasyon sorunundan, enerji altyapısının bütünlüğünü etkileyen bir sistemik zafiyete evrilmiştir. Bu nedenle, proaktif modernizasyon ve gelişmiş, adaptif savunma sistemlerinin zorunlu kılınması, EV şarj ağlarının hem finansal hem de operasyonel sürekliliği için stratejik bir zorunluluk teşkil etmektedir.

Alıntılanan çalışmalar

1. Understanding OCPP Security Profiles: Securing the Future of EV Charging - eDRV, erişim tarihi Kasım 3, 2025, https://www.edrv.io/blog/understanding-ocpp-security-profiles
2. OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison - Ampcontrol, erişim tarihi Kasım 3, 2025, https://www.ampcontrol.io/post/ocpp-1-6-vs-ocpp-2-0-a-comprehensive-comparison

3. OCPP (Open Charge Point Protocol), erişim tarihi Kasım 3, 2025, https://openchargealliance.org/protocols/open-charge-point-protocol/
4. OCPP Protocols (OCPP 1.6, OCPP 2.0.1, and OCPP 2.1) - Tridens, erişim tarihi Kasım 3, 2025, https://tridenstechnology.com/ocpp-protocol/
5. Federated detection of open charge point protocol 1.6 cyberattacks, erişim tarihi Kasım 3, 2025, https://www.oaepublish.com/articles/ces.2025.04
6. CVE-2024-23971 Detail - NVD, erişim tarihi Kasım 3, 2025, https://nvd.nist.gov/vuln/detail/CVE-2024-23971
7. Open Charge Point Protocol 1.6 - The ASRG Garage, erişim tarihi Kasım 3, 2025, https://garage.asrg.io/wp-content/uploads/sites/2/2024/04/ocpp-1.6.pdf
8. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - - INL Research Library Digital Repository - Idaho National Laboratory, erişim tarihi Kasım 3, 2025, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65949.pdf
9. MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations - NTU > IRep, erişim tarihi Kasım 3, 2025, https://irep.ntu.ac.uk/id/eprint/54419/1/2478037_Brown.pdf
10. — OCPP 1.6 Implementation Overview - ABB, erişim tarihi Kasım 3, 2025, https://library.e.abb.com/public/93260d686761440fa855adc4c722857f/ABB_Terra_AC_Charger_OCPP1.6_ImplementationOverview%20_FW1.8.34.pdf?x-sign=WTORgSlmdlZSfvRVnJfQx5PYCqqKh3oRBB%2BuZUB1%2F0HGF55XBh6VTmSaGwmK2Unt