Temel Makale :
OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0

Temel Makalenin Analizi

- **Ele alınan temel sorun:** Elektrikli araç şarj istasyonlarında kullanılan en güncel protokol olan OCPP-v2.0.1'in, içerdiği yeni güvenlik önlemlerine rağmen siber ve fiziksel tehditlere karşı hala savunmasız olup olmadığının incelenmesidir.
- **Kullanılan yöntem:** Tehditleri tanımlamak ve sınıflandırmak için STRIDE (tehdit analizi metodolojisi) uyarlanmış ve risk değerlendirmesi yapmak için bu metodoloji DREAD (risk değerlendirme modeli) ile birleştirilmiştir.
- **Ulaşılan ana sonuç:** Analizler, OCPP-v2.0.1'in önceki sürümlere göre gelişmiş olmasına rağmen, potansiyel güvenlik risklerinin hala devam ettiğini ve gelecekte daha fazla koruma önlemi gerektirdiğini göstermektedir.

(Yani kısacası, önce "ne tür sorunlar olabilir?" diye baktılar (STRIDE), sonra da "bu sorunlar ne kadar ciddi?" diye ölçtüler (DREAD).)

"Ne tür sorunlar olabilir?"

STRIDE (Tehdit Modellemesi):

- Bu, bir sisteme (bir yazılıma, bir ağa veya o makaledeki gibi bir şarj istasyonuna) ne tür saldırılar olabileceğini sistematik olarak bulmaya yarayan bir yöntemdir.
- Adı, altı ana tehdit kategorisinin baş harflerinden oluşan bir kısaltmadır:
  - **S**poofing (Kimlik Sahtekarlığı)
  - **T**ampering (Veri Bozma veya Kurcalama)
  - **R**epudiation (İnkar Etme, bir işlemi yaptığını reddetme)
  - **I**nformation Disclosure (Bilgi İfşası, gizli verilerin sızdırılması)
  - **D**enial of Service (Hizmet Reddi, sistemi çalışmaz hale getirme)
  - **E**levation of Privilege (Yetki Yükseltme, normal bir kullanıcının admin yetkilerine ulaşması)
- **Amacı:** Güvenlik uzmanları bu listeyi kullanarak "Sistemimizde 'Kimlik Sahtekarlığı' açığı var mı? 'Veri Bozma' açığı var mı?" diye tek tek kontrol ederler. Hiçbir olasılığı atlamamalarını sağlar.

"Bulduğumuz bu sorunlar ne kadar ciddi?"

DREAD (Risk Derecelendirmesi):

- Bu, STRIDE ile bulduğunuz tehditleri önceliklendirmeye yarayan bir modeldir. Yani, "Tamam, 10 tane tehdit bulduk ama hangisi en tehlikeli? Hangisini ilk önce düzeltmeliyiz?" sorusuna cevap verir.
- Bu da bir kısaltmadır ve bir tehdidin ciddiyetini ölçen 5 faktörden oluşur:
  - **D**amage (Hasar potansiyeli: Bu saldırı olursa ne kadar kötü olur?)
  - **R**eproducibility (Tekrarlanabilirlik: Saldırıyı kopyalamak ne kadar kolay?)
  - **E**xploitability (Sömürülebilirlik: Bu açığı kullanmak ne kadar kolay?)
  - **A**ffected users (Etkilenen kullanıcılar: Saldırı olursa kaç kişi etkilenir?)
  - **D**iscoverability (Keşfedilebilirlik: Bu açığı bulmak ne kadar kolay?)
- **Amacı:** Her tehdide bu 5 kategori üzerinden 1-10 arası bir puan verilir ve ortalaması alınır. Puanı en yüksek olan tehdit, en yüksek riski taşır ve ilk önce o düzeltilir.

Makalenin Amacı ve Kapsamı

Bu makale, elektrikli araç (EV) şarj istasyonlarında (CS) kullanılan en güncel iletişim protokolü olan OCPP-v2.0.1'i güvenlik açısından analiz etmektedir. Önceki sürümlerde bulunan güvenlik açıklarını kapatmak için bu yeni protokole birçok güvenlik özelliği eklenmiştir. Ancak araştırmacılar, bu yeni sürümün bile, özellikle de bu istasyonlar mikro şebekelere (microgrids) bağlandığında, siber ve fiziksel saldırılara karşı hala savunmasız olup olmadığını belirlemeyi amaçlamıştır.

Kullanılan Yöntem: STRIDE + DREAD

Araştırmacılar, bu güvenlik analizini yapmak için daha önce konuştuğumuz iki metodolojiyi birleştirip özel bir model oluşturmuştur:

1. **STRIDE (Tehdit Modellemesi):** Önce, bir şarj istasyonu sistemine (kullanıcılar, şarj istasyonu, merkezi yönetim sistemi, enerji yönetim sistemi) ne tür saldırılar olabileceğini sınıflandırmak için STRIDE modelini kullanmışlardır. Bu modeli, sadece siber (kontrol) varlıkları değil, aynı zamanda fiziksel (enerji) varlıkları da kapsayacak şekilde genişletmişlerdir.
2. **DREAD (Risk Değerlendirmesi):** STRIDE ile "neler olabilir?" sorusunu yanıtladıktan sonra, buldukları her bir tehdidin "ne kadar ciddi?" olduğunu ölçmek için DREAD modelini kullanmışlardır. Her tehdidi Hasar (Damage), Tekrarlanabilirlik (Reproducibility), Sömürülebilirlik (Exploitability), Etkilenen Kullanıcılar (Affected users) ve Keşfedilebilirlik (Discoverability) kriterlerine göre 1-10 arası puanlamışlardır.

Tespit Edilen Ana Tehditler ve Riskler

Analiz sonucunda, OCPP-v2.0.1 protokolünün hala ciddi riskler barındırdığı ortaya çıkmıştır. En yüksek risk puanına sahip (en tehlikeli) tehditler şunlardır:

1-**Hizmet Reddi (Denial of Service - DoS) - (Risk Puanı: 9.2/10):**Bu, en yüksek riskli tehdit olarak belirlenmiştir. Bir saldırganın, şarj istasyonunu (CS), merkezi yönetim sistemini (CSMS) veya enerji yönetim sistemini (EMS) kilitleyerek veya yavaşlatarak kullanıcıların araçlarını şarj etmesini engellemesidir. Bu, kalp atışı (heartbeat) mesajlarını manipüle ederek veya sistemi çevrimdışı moda girmeye zorlayarak yapılabilir.

2-**OCPP Yapılandırma Değişkenlerini Kurcalama (Tampering) - (Risk Puanı: 8.6/10):**İkinci en yüksek risk, bir saldırganın şarj istasyonunun ayarlarını (Configuration Variables - CVs) değiştirmesidir. Örneğin, saldırgan "meterValues" (sayaç değeri) verisini değiştirerek enerji hırsızlığı yapabilir (TC-7) veya akıllı şarj profillerini değiştirerek enerji şebekesinin dengesini bozabilir (TC-8).

3-**Şarj İstasyonu Kimlik Sahtekarlığı (CS Spoofing) - (Risk Puanı: 8.0/10):**Saldırganın, şarj istasyonunu taklit ederek merkezi sisteme bağlanmasıdır. Bunu yapabilmek için istasyonun kimlik bilgilerini (şifre, sertifika vb.) çalması gerekir. Şarj istasyonları halka açık yerlerde bulunduğu için , saldırganların bu bilgilere fiziksel erişimle ulaşması (cihazı açıp içindeki depolama biriminden çalması) büyük bir olasılıktır.

Ana Sonuç ve Çözüm Önerileri

Ana Sonuç: Makalenin vardığı temel sonuç şudur: OCPP-v2.0.1'deki yeni güvenlik önlemleri (şifreleme, sertifikalar vb.) iyi bir gelişme olsa da, tek başlarına yeterli değildir. Protokolün en zayıf noktası, bütünlük (verilerin değiştirilmemesi) ve erişilebilirlik (sistemin çalışır durumda kalması) gereksinimleridir. En büyük riskler, şarj istasyonlarının halka açık, gözetimsiz yerlerde bulunmasından ve fiziksel saldırılara açık olmasından kaynaklanmaktadır.

Başlıca Çözüm Önerileri: Araştırmacılar, bu yüksek riskli tehditleri azaltmak için şu önlemleri önermektedir:

- **En Yüksek Güvenlik Profilini Zorunlu Kılma:** Protokolün en güvenli modu olan "Security Profile 3" (karşılıklı kimlik doğrulamalı TLS v1.3 sertifikaları) kullanımının zorunlu hale getirilmesi.
- **Bütünlük Doğrulaması:** Tüm önemli verilerin ve yapılandırma dosyalarının değiştirilmediğinden emin olmak için dijital imzalar ve hash (örn. SHA-256) fonksiyonlarının kullanılması.
- **Anomali Tespiti:** DoS saldırılarını veya şüpheli davranışları tespit etmek için Makine Öğrenimi (ML) algoritmaları kullanan gelişmiş izleme sistemlerinin (SIEM gibi) kurulması.
- **Yedeklilik (Redundancy):** Bir bağlantı koptuğunda veya sistem çöktüğünde bile şarj işleminin devam etmesini sağlayacak yedek iletişim kanalları ve sistemlerin (proxy'ler gibi) kullanılması.

Terimler Sözlüğü

OCPP (Open Charge Point Protocol - Açık Şarj Noktası Protokolü): Şarj İstasyonları (CS) ile bu istasyonları yöneten Merkezi Yönetim Sistemi (CSMS) arasındaki iletişimi kuran standart bir uygulama protokolüdür.
CS (Charging Station - Şarj İstasyonu): Elektrikli araçların (EV) şarj edildiği fiziksel istasyonlar.
CSMS (Charging Station Management System - Şarj İstasyonu Yönetim Sistemi): Genellikle halka açık yerlerde bulunan tüm şarj istasyonlarındaki işlemleri ve kullanıcı taleplerini verimli bir şekilde yönetmekten sorumlu merkezi sistemdir.
EVSE (Electric Vehicle Supply Equipment - Elektrikli Araç Besleme Ekipmanı): Şarj istasyonunun (CS) içinde bulunan ve elektrikli araçla (EV) fiziksel bağlantıyı ve iletişimi başlatan/durduran parçalardır.
ISO 15118: Elektrikli araç (EV) ile şarj istasyonu (CS) arasındaki çift yönlü iletişimi (V2G - Araçtan Şebekeye) destekleyen uluslararası bir standarttır.
CV (Configuration Variables - Yapılandırma Değişkenleri): Şarj istasyonunun nasıl çalışacağını belirleyen ayar parametreleridir. Makale, bu değişkenlerin (CVs) saldırganlar tarafından değiştirilmeye (tampering) açık olduğunu belirtiyor.

Terimler sözlüğünün devamı word dosyasında mevcuttur.