**1. RAPOR: WebSocket/OCPP Mesaj Fuzzing ile Hizmet Reddi (DoS)**

**1. Senaryo Özeti**

Saldırgan, Şarj İstasyonuna (CS) veya Şarj İstasyonu Yönetim Sistemine (CSMS) WebSocket bağlantısı üzerinden kötü biçimlendirilmiş (malformed) veya beklenmedik (fuzzing) OCPP mesajları göndererek hedef sistemin kaynaklarını tüketmeyi, kararsız hale getirmeyi veya tamamen çökertmeyi amaçlar.

**2. Hedef Varlıklar**

Birincil Hedef: OCPP mesajlarını işleyen CS veya CSMS'nin WebSocket/JSON ayrıştırma motoru. İkincil Hedefler: Şarj hizmetinin sürekliliği, sunucunun/istasyonun çalışma süresi.

**3. İlgili Zafiyetler**

OCPP mesajlarının (JSON) ayrıştırılmasında (parsing) ve işlenmesinde yetersiz hata kontrolü; WebSocket bağlantı yönetiminde zafiyetler; kaynak tüketimi limitlerinin (CPU/Bellek) yetersizliği.

**4. Tehdit Kategorisi**

STRIDE: Denial of Service (DoS), Tampering (Bazı varyantlarda).

**5. Saldırı Vektörü ve Adımları**

1.Bağlantı Kurma: Saldırgan, hedef CS veya CSMS ile geçerli bir WebSocket bağlantısı kurar.

2.Fuzzing: Bağlantı üzerinden, OCPP protokolünün beklediği JSON yapısını bozacak şekilde, aşırı uzun, hatalı veri tipleri içeren veya geçerli olmayan alan adlarına sahip mesajlar gönderilir.

3.Kaynak Tüketimi: Hatalı mesajlar, hedef sistemin ayrıştırma motorunda sonsuz döngülere, bellek taşmalarına veya aşırı CPU kullanımına neden olur.

4.Hizmet Reddi: Sistem, geçerli OCPP mesajlarını işlemeyi durdurur veya tamamen çöker, böylece şarj hizmeti kesintiye uğrar.

**8. İlgili Karşı Önlemler**

Gelen OCPP mesajlarında katı JSON şeması doğrulaması (validation); WebSocket bağlantıları için kaynak limitleri (rate limiting); OCPP 2.0.1'in daha sağlam hata işleme mekanizmalarını kullanma.

Kaynak:

•Elmo, D., et al. (2023). Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MitM, and Code Injection Exploits Using OCPP 1.6. IEEE Xplore. (DoS ve RCE potansiyeli)

**2. RAPOR: Yetkisiz Şarj Oturumu (Unauthorized Charging)**

**1. Senaryo Özeti**

Saldırgan, zayıf kimlik doğrulama mekanizmalarını kullanarak (örneğin, tahmin edilebilir ID Tag'ler, zayıf fiziksel erişim kontrolü veya replay saldırıları) yetkisi olmayan bir şarj oturumu başlatır ve enerji hırsızlığı yapar.

**2. Hedef Varlıklar**

Birincil Hedef: Şarj İstasyonu (CS) ve kimlik doğrulama (Authentication) süreci. İkincil Hedefler: Faturalama sistemi, enerji sağlayıcısı.

**3. İlgili Zafiyetler**

Tahmin edilebilir ID Tag'ler (RFID kart numaraları); yetersiz oturum yönetimi (ID Tag'in bir kez kullanıldıktan sonra geçersiz kılınmaması); fiziksel güvenlik eksikliği; OCPP 1.6'da Authorize isteğinin şarj işlemini başlatmadan önce yeterince sıkı kontrol edilmemesi.

**4. Tehdit Kategorisi**

STRIDE: Spoofing (Taklit), Tampering (Faturalama verilerinde).

**5. Saldırı Vektörü ve Adımları**

1.Bilgi Toplama: Saldırgan, geçerli bir kullanıcıya ait ID Tag'i (örneğin, yere düşmüş bir RFID kartından veya ağ dinlemesiyle) ele geçirir.

2.Taklit: Saldırgan, ele geçirdiği ID Tag'i kullanarak şarj istasyonuna bir Authorize isteği gönderir.

3.Oturum Başlatma: CSMS, bu ID Tag'i geçerli kabul eder ve CS'ye RemoteStartTransaction veya yerel olarak şarjı başlatma izni verir.

4.Enerji Hırsızlığı: Saldırgan, yetkisiz olarak şarj oturumunu tamamlar ve enerji tüketiminin faturasını gerçek kullanıcıya veya sisteme yükler.

**8. İlgili Karşı Önlemler**

ID Tag'ler için güçlü şifreleme ve karmaşık yapılar kullanma; her oturum için tek kullanımlık token'lar (nonce) veya dinamik ID'ler kullanma; OCPP 2.0.1'in gelişmiş güvenlik profillerini (örneğin, Plug & Charge veya mTLS ile kullanıcı kimlik doğrulaması) kullanma.

Kaynak:

•Hamdare, S., et al. (2025). Cyber defense in OCPP for EV charging security risks. Springer. (Yetkisiz şarj ve Spoofing tehditleri)

**3. RAPOR: CSMS Taklidi (Spoofing) ile CS Kontrolünün Ele Geçirilmesi**

**1. Senaryo Özeti**

Saldırgan, Şarj İstasyonu Yönetim Sistemini (CSMS) taklit ederek Şarj İstasyonuna (CS) bağlanır ve istasyonun kritik ayarlarını değiştirir (örneğin, SetConfiguration), şarjı durdurur (RemoteStopTransaction) veya istasyonu kalıcı olarak devre dışı bırakır.

**2. Hedef Varlıklar**

Birincil Hedef: CS'nin CSMS'nin kimliğini doğrulama mekanizması (veya eksikliği). İkincil Hedefler: CS'nin operasyonel ayarları, hizmet sürekliliği.

**3. İlgili Zafiyetler**

CS'nin CSMS'nin kimliğini doğrulamak için Karşılıklı TLS (mTLS) kullanmaması; zayıf veya varsayılan kimlik bilgileri; ağ segmentasyonu eksikliği; CS'nin yalnızca IP adresi veya DNS adına güvenmesi.

**4. Tehdit Kategorisi**

STRIDE: Spoofing (Taklit), Tampering (Kurcalama), Denial of Service (DoS).

**5. Saldırı Vektörü ve Adımları**

1.Keşif: Saldırgan, hedef CS'nin CSMS'ye bağlanmak için kullandığı adresi ve portu belirler.

2.Taklit Ortamı: Saldırgan, kendisini gerçek CSMS gibi gösterecek bir sunucu kurar ve CS'nin bağlantı adresini manipüle eder (örneğin, DNS zehirlenmesi veya ARP Spoofing).

3.Bağlantı Kurma: CS, saldırganın sahte CSMS'sine bağlanır.

4.Kötü Amaçlı Komutlar: Saldırgan, CS'ye SetConfiguration (örneğin, şarj limitini sıfırlama), RemoteStopTransaction veya Reset gibi yetkili komutlar göndererek istasyonun kontrolünü ele geçirir.

**8. İlgili Karşı Önlemler**

CS ve CSMS arasında Karşılıklı TLS (mTLS) kullanımı zorunluluğu; CS'de yalnızca güvenilir CSMS sertifikalarının kabul edilmesi (sertifika sabitleme/pinning); ağ segmentasyonu ve erişim kontrol listeleri (ACL).

Kaynak:

•Open Charge Alliance. OCPP 2.0.1 Security Whitepaper. (mTLS ve sertifika sabitleme gereksinimleri)

**4. RAPOR: MeterValue Kurcalaması ile Faturalama Manipülasyonu**

**1. Senaryo Özeti**

Saldırgan, Şarj İstasyonunun (CS) Şarj İstasyonu Yönetim Sistemine (CSMS) gönderdiği enerji tüketim verilerini (MeterValues) yakalar ve değiştirir. Amaç, şarj maliyetini düşürmek (enerji hırsızlığı) veya rakip kullanıcılara/şirketlere yüksek fatura çıkarmaktır.

**2. Hedef Varlıklar**

Birincil Hedef: CS'nin ölçüm cihazı (meter) ve MeterValues mesajının bütünlüğü. İkincil Hedefler: Faturalama sistemi, finansal verilerin güvenilirliği.

**3. İlgili Zafiyetler**

OCPP mesajlarının uçtan uca bütünlük kontrolünün eksikliği; MitM saldırılarına karşı zayıf iletişim güvenliği; ölçüm cihazının fiziksel olarak kurcalanabilir olması; CSMS'nin gelen MeterValues verilerinin mantıksal geçerliliğini kontrol etmemesi.

**4. Tehdit Kategorisi**

STRIDE: Tampering (Kurcalama), Repudiation (İnkar), Spoofing (Veri Taklidi).

**5. Saldırı Vektörü ve Adımları**

1.Erişim: Saldırgan, CS ile CSMS arasındaki iletişime araya girer (MitM) veya CS'nin yerel ağına erişim sağlar.

2.Yakala ve Değiştir: Saldırgan, şarj oturumu sırasında CS'den CSMS'ye gönderilen MeterValues mesajlarını yakalar.

3.Manipülasyon: Saldırgan, mesajdaki meterValue alanını, gerçek tüketimden daha düşük (kendi faturasını düşürmek için) veya daha yüksek (başkasına zarar vermek için) bir değerle değiştirir.

4.İletme: Değiştirilen mesaj CSMS'ye iletilir ve CSMS bu sahte veriyi faturalama için kullanır.

**8. İlgili Karşı Önlemler**

OCPP 2.0.1'in uçtan uca güvenlik mekanizmalarını kullanma; ölçüm cihazı verilerinin uygulama düzeyinde dijital olarak imzalanması (örneğin, DSMR standardı veya benzeri); CSMS'de mantıksal doğrulama (örneğin, maksimum şarj gücünü aşan tüketim değerlerini reddetme).

Kaynak:

•Boussaha, S., et al. (2025). EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing. USENIX. (Veri bütünlüğü ve gizliliği)

**5. RAPOR: Tedarik Zinciri Saldırısı (Supply Chain Attack)**

**1. Senaryo Özeti**

Saldırgan, şarj istasyonu donanımının veya yazılımının üretim, dağıtım veya kurulum aşamasında cihaza kötü amaçlı yazılım (malware) veya arka kapı (backdoor) enjekte eder. Bu, istasyonun henüz sahaya çıkmadan tehlikeye atılması anlamına gelir.

**2. Hedef Varlıklar**

Birincil Hedef: Şarj istasyonunun donanımı ve fabrika çıkışlı firmware'i. İkincil Hedefler: Tüm şarj ağı (CSMS ve diğer CS'ler), tedarikçi firmanın itibarı.

**3. İlgili Zafiyetler**

Üretim tesislerinde zayıf fiziksel güvenlik; firmware geliştirme ve yayınlama süreçlerinde yetersiz güvenlik denetimi; cihazların ağa ilk bağlandığında otomatik olarak güncelleme/doğrulama yapmaması.

**4. Tehdit Kategorisi**

STRIDE: Tampering (Kurcalama), Spoofing (Taklit), Information Disclosure (Bilgi Açığa Çıkarma).

**5. Saldırı Vektörü ve Adımları**

1.Enjeksiyon: Saldırgan, tedarik zincirinin erken bir aşamasında (örneğin, firmware derleme sunucusunda veya donanım montajında), cihazın işletim sistemine kalıcı bir arka kapı yerleştirir.

2.Dağıtım: Tehlikeli cihaz, normal bir ürün gibi sahaya kurulur ve CSMS'ye bağlanır.

3.Aktivasyon: Arka kapı, saldırganın komutunu bekler veya belirli bir tetikleyici (örneğin, belirli bir tarih) ile aktif hale gelir.

4.Kontrol: Saldırgan, arka kapı üzerinden şarj istasyonuna doğrudan erişim sağlar, OCPP protokolünü atlayarak istasyonu manipüle eder.

**8. İlgili Karşı Önlemler**

Güvenilir Önyükleme (Trusted Boot) mekanizmaları; donanım tabanlı güvenlik modülleri (TPM); tedarikçi firmalarla sıkı güvenlik denetimleri; ağa ilk bağlandığında otomatik güvenlik güncellemesi ve sertifika doğrulama.

Kaynak:

•SaiFlow Research Team. (Blog). Exploiting Hidden Supply-Chain Vulnerabilities to Attack EV Chargers and CPOs. (Tedarik zinciri saldırı vektörleri)

**6. RAPOR: Yüksek Yoğunluklu Eşzamanlı Şarj İsteği ile Şebeke İstikrarsızlığı**

**1. Senaryo Özeti**

Saldırgan, birçok Şarj İstasyonuna (CS) aynı anda ve senkronize bir şekilde şarj oturumu başlatma komutu (RemoteStartTransaction) göndererek yerel elektrik şebekesinde veya trafo merkezinde ani ve kontrolsüz bir yük artışı (Load Spike) yaratmayı amaçlar.

**2. Hedef Varlıklar**

Birincil Hedef: Şarj İstasyonu Yönetim Sistemi (CSMS) ve Yük Yönetimi (Load Management) sistemi. İkincil Hedefler: Yerel elektrik şebekesi, trafo merkezleri, şebeke operatörünün güvenilirliği.

**3. İlgili Zafiyetler**

CSMS'de yetersiz Yük Yönetimi (Smart Charging) kısıtlamaları; RemoteStartTransaction komutunun toplu olarak ve hızlı bir şekilde işlenmesinde zafiyet; şarj istasyonlarının coğrafi dağılımının ve şebeke kapasitesinin göz ardı edilmesi.

**4. Tehdit Kategorisi**

STRIDE: Denial of Service (DoS - Şebeke seviyesinde).

**5. Saldırı Vektörü ve Adımları**

1.Kontrol Ele Geçirme: Saldırgan, bir dizi CS'nin veya CSMS'nin bir kısmının kontrolünü ele geçirir (örneğin, zayıf kimlik bilgileri veya MitM ile).

2.Senkronizasyon: Saldırgan, kontrol ettiği tüm CS'lere aynı anda şarj oturumu başlatma komutunu gönderecek bir zamanlayıcı ayarlar.

3.Yük Yaratma: Belirlenen anda, yüzlerce veya binlerce şarj istasyonu aynı anda maksimum güçle şarj etmeye başlar.

4.Şebeke Etkisi: Yerel şebeke, bu ani ve senkronize yük artışını kaldıramaz ve voltaj düşüşleri, frekans dalgalanmaları veya trafo arızaları meydana gelir.

**8. İlgili Karşı Önlemler**

OCPP 2.0.1'in gelişmiş Smart Charging (Yük Yönetimi) özellikleri; RemoteStartTransaction istekleri için oran sınırlaması (rate limiting); şebeke operatörleriyle entegre yük dengeleme algoritmaları; coğrafi olarak dağıtılmış CS'ler için toplu komutların geciktirilerek gönderilmesi.

Kaynak:

•Sayed, M. A. (2024). Tackling the Electric Vehicle-Related Threats to Power Grid Stability. Core.ac.uk. (Toplu şarj ile şebeke istikrarsızlığı)

**7. RAPOR: İzinsiz Veri Açığa Çıkarma (Information Disclosure)**

**1. Senaryo Özeti**

Saldırgan, OCPP iletişimini dinleyerek (eavesdropping) veya CSMS'ye yetkisiz erişim sağlayarak hassas kullanıcı verilerini, faturalama kayıtlarını, şarj istasyonu konumlarını veya CSMS'nin kritik yapılandırma bilgilerini ele geçirir.

**2. Hedef Varlıklar**

Birincil Hedef: OCPP mesajları (özellikle OCPP 1.6'da şifrelenmemiş uygulamalar). İkincil Hedefler: Kullanıcıların kişisel verileri (PII), şarj alışkanlıkları, ödeme bilgileri.

**3. İlgili Zafiyetler**

TLS/SSL şifrelemesinin kullanılmaması veya yanlış yapılandırılması; zayıf şifreleme algoritmaları; CSMS'de yetersiz erişim kontrolü; log dosyalarının şifrelenmemiş hassas veriler içermesi.

**4. Tehdit Kategorisi**

STRIDE: Information Disclosure (Bilgi Açığa Çıkarma).

**5. Saldırı Vektörü ve Adımları**

1.Dinleme: Saldırgan, CS ile CSMS arasındaki ağ trafiğini dinler (örneğin, kablosuz ağa sızarak veya ağ cihazlarına fiziksel erişim sağlayarak).

2.Veri Yakalama: Eğer iletişim şifrelenmemişse (HTTP yerine HTTPS/WSS kullanılmıyorsa), saldırgan Authorize, StartTransaction, StopTransaction gibi mesajlardaki ID Tag'leri, şarj sürelerini ve konum bilgilerini yakalar.

3.Analiz: Saldırgan, elde ettiği verileri analiz ederek kullanıcıların günlük rutinlerini, ev ve iş adreslerini veya finansal bilgilerini (ID Tag'den yola çıkarak) belirler.

**8. İlgili Karşı Önlemler**

TLS 1.3 veya daha üstünü kullanarak tüm OCPP iletişimini şifreleme zorunluluğu; hassas verilerin (örneğin, ID Tag'ler) uygulama düzeyinde hashlenmesi veya şifrelenmesi; CSMS'de güçlü erişim kontrolü ve yetkilendirme mekanizmaları.

Kaynak:

•Boussaha, S., et al. (2025). EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing. USENIX. (Veri gizliliği ve bilgi açığa çıkarma)

**8. RAPOR: İletişim Kesintisi ile İnkar (Repudiation) Saldırısı**

**1. Senaryo Özeti**

Saldırgan, bir şarj oturumunun gerçekleştiğine veya belirli bir komutun gönderildiğine dair kanıtları ortadan kaldırmak için OCPP mesajlarını siler veya değiştirir. Amaç, şarj oturumunu inkar etmek ve faturalandırmadan kaçınmaktır.

**2. Hedef Varlıklar**

Birincil Hedef: CSMS ve CS'nin log kayıtları ve oturum veritabanı. İkincil Hedefler: Faturalama kayıtları, yasal kanıtlar.

**3. İlgili Zafiyetler**

OCPP mesajlarının uygulama düzeyinde dijital olarak imzalanmaması; logların merkezi ve güvenli bir şekilde saklanmaması; CSMS'nin oturum verilerinin bütünlüğünü koruyamaması.

**4. Tehdit Kategorisi**

STRIDE: Repudiation (İnkar).

**5. Saldırı Vektörü ve Adımları**

1.Şarj Etme: Saldırgan, yetkili bir şekilde şarj oturumunu başlatır ve tamamlar.

2.Veri Manipülasyonu: Saldırgan, şarj oturumuna ait StartTransaction, MeterValues ve StopTransaction mesajlarının CSMS'ye ulaşmasını engeller (MitM ile siler) veya CS'nin yerel loglarını siler.

3.İnkar: Saldırgan, fatura geldiğinde şarj oturumunu inkar eder ve sistemde bu oturumun gerçekleştiğine dair güvenilir, değiştirilemez bir kanıt bulunamaz.

**8. İlgili Karşı Önlemler**

OCPP 2.0.1'in gelişmiş güvenlik özellikleri; tüm kritik OCPP mesajlarının (özellikle faturalama ile ilgili olanların) uygulama düzeyinde dijital olarak imzalanması; güvenli, merkezi ve değiştirilemez loglama (Secure Logging).

Kaynak:

•Alcaraz, C., et al. (2017). OCPP protocol: Security threats and challenges. IEEE Xplore. (İnkar saldırıları ve protokol zafiyetleri)

**9. RAPOR: Zayıf Parola/Kimlik Bilgisi ile Yetkisiz Erişim**

**1. Senaryo Özeti**

Saldırgan, Şarj İstasyonunun (CS) veya CSMS'nin web arayüzünün/API'sinin varsayılan, zayıf veya kolayca tahmin edilebilen kimlik bilgilerini (parola, API anahtarı) kullanarak sisteme yetkisiz erişim sağlar.

**2. Hedef Varlıklar**

Birincil Hedef: CS'nin yerel yönetici arayüzü, CSMS'nin yönetici paneli veya API erişimi. İkincil Hedefler: Tüm ağ yapılandırması, kullanıcı verileri.

**3. İlgili Zafiyetler**

Varsayılan veya fabrika şifrelerinin değiştirilmemesi; zayıf parola politikaları (kısa, basit parolalar); kaba kuvvet (brute-force) saldırılarına karşı yetersiz koruma (oran sınırlaması eksikliği).

**4. Tehdit Kategorisi**

STRIDE: Spoofing (Taklit), Information Disclosure (Bilgi Açığa Çıkarma), Tampering (Kurcalama).

**5. Saldırı Vektörü ve Adımları**

1.Keşif: Saldırgan, hedef CSMS'nin veya CS'nin yönetim arayüzünü bulur.

2.Kimlik Bilgisi Denemeleri: Saldırgan, yaygın varsayılan şifreleri (örneğin, admin/admin, root/123456) veya kaba kuvvet araçlarını kullanarak giriş yapmaya çalışır.

3.Yetkisiz Erişim: Başarılı girişten sonra, saldırgan sistemin tüm yapılandırmasına erişir.

4.Kötü Amaçlı Eylem: Saldırgan, CS'nin OCPP bağlantı adresini değiştirir (kendi sahte CSMS'sine yönlendirir), faturalama ayarlarını manipüle eder veya kullanıcı verilerini çalar.

**8. İlgili Karşı Önlemler**

Kurulum sırasında varsayılan şifrelerin zorunlu olarak değiştirilmesi; güçlü parola politikaları ve çok faktörlü kimlik doğrulama (MFA); başarısız giriş denemeleri için oran sınırlaması ve hesap kilitleme.

Kaynak:

•SEC Consult. (Vulnerability Lab Advisory). Multiple Vulnerabilities in eCharge Hardy Barth cPH2 and cpp2 Charging Stations. (Zayıf kimlik bilgisi örnekleri)

**10. RAPOR: CS'nin Fiziksel Kurcalanması ile Ağ Erişimi**

**1. Senaryo Özeti**

Saldırgan, Şarj İstasyonuna (CS) fiziksel erişim sağlayarak (örneğin, servis panelini açarak) istasyonun içindeki ağ portlarına veya USB/seri portlarına yetkisiz cihazlar (örneğin, ağ dinleme cihazları, 4G modemler) bağlar ve böylece iç ağa sızar.

**2. Hedef Varlıklar**

Birincil Hedef: Şarj İstasyonunun fiziksel güvenliği (kilitler, mühürler). İkincil Hedefler: CS'nin bağlı olduğu yerel ağ, diğer CS'ler ve CSMS.

**3. İlgili Zafiyetler**

Zayıf fiziksel kilitler veya kolayca açılabilen servis panelleri; iç ağ portlarının (Ethernet, USB) devre dışı bırakılmaması veya izlenmemesi; ağ segmentasyonu eksikliği (CS'nin bağlı olduğu ağın diğer kritik sistemlerle aynı olması).

**4. Tehdit Kategorisi**

STRIDE: Tampering (Kurcalama), Information Disclosure (Bilgi Açığa Çıkarma), Spoofing (Taklit).

**5. Saldırı Vektörü ve Adımları**

1.Fiziksel Erişim: Saldırgan, bir tornavida veya anahtar seti ile CS'nin servis panelini açar.

2.Cihaz Bağlama: Saldırgan, CS'nin içindeki Ethernet kablosunu keser ve araya kendi ağ dinleme cihazını (tap) veya bir Raspberry Pi gibi sızma cihazını yerleştirir.

3.Ağ Sızması: Saldırgan, bu cihaz üzerinden CS'nin bağlı olduğu yerel ağa erişim sağlar ve ağdaki diğer CS'leri veya CSMS'yi hedef almaya başlar.

**8. İlgili Karşı Önlemler**

Yüksek güvenlikli kilitler ve kurcalama sensörleri; iç ağ portlarının fiziksel olarak devre dışı bırakılması (kullanılmıyorsa); CS'lerin yalnızca kendi VLAN'larında (ağ segmentasyonu) izole edilmesi; ağ erişim kontrolü (NAC) ile yetkisiz cihazların engellenmesi.

Kaynak:

•Brown, S., et al. (2025). MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations. NTU. (Fiziksel erişim ve ağ sızması)

**11. RAPOR: OCPP Mesajlarının Tekrarı (Replay Attack)**

**1. Senaryo Özeti**

Saldırgan, geçerli bir OCPP mesajını (örneğin, başarılı bir Authorize veya RemoteStartTransaction mesajını) yakalar ve daha sonra aynı mesajı tekrar göndererek yetkisiz bir eylem gerçekleştirir.

**2. Hedef Varlıklar**

Birincil Hedef: CS ve CSMS'nin mesaj işleme mekanizması. İkincil Hedefler: Yetkilendirme süreci.

**3. İlgili Zafiyetler**

OCPP mesajlarında tek kullanımlık rastgele sayıların (nonce) veya zaman damgalarının (timestamp) kullanılmaması; CSMS'nin daha önce işlenmiş mesajları tespit edememesi.

**4. Tehdit Kategorisi**

STRIDE: Spoofing (Taklit), Tampering (Kurcalama).

**5. Saldırı Vektörü ve Adımları**

1.Yakala: Saldırgan, geçerli bir kullanıcının Authorize mesajını yakalar.

2.Tekrar Gönder: Kullanıcı ayrıldıktan sonra, saldırgan yakaladığı mesajı tekrar CS'ye gönderir.

3.Yetkisiz İşlem: CS, bu mesajı yeni ve geçerli bir yetkilendirme olarak kabul eder ve saldırganın şarj oturumu başlatmasına izin verir.

**8. İlgili Karşı Önlemler**

Tüm kritik OCPP mesajlarına tek kullanımlık rastgele sayılar (nonce) eklenmesi ve CSMS'nin bu nonce'ları takip etmesi; mesajların zaman damgalarını içermesi ve eski mesajların reddedilmesi.

Kaynak:

•Hamdare, S., et al. (2025). Cyber defense in OCPP for EV charging security risks. Springer. (Replay saldırıları ve karşı önlemleri)