# RAPOR: BootNotification Manipülasyonu

## 1. Senaryo Özeti

Şarj İstasyonu (Charge Point - CP) tarafından merkezi sisteme (Charge Point Central System - CSMS) gönderilen BootNotification mesajının (OCPP üzerinden WebSocket/JSON) manipüle edilmesiyle ortaya çıkan bir anomali senaryosudur. Saldırgan, BootNotification içindeki alanları (ör. chargePointModel, chargePointVendor, chargePointSerialNumber, firmwareVersion, heartbeatInterval) geçersiz, beklenmedik veya tekrarlı şekilde göndererek CSMS tarafında kayıt, bağlantı durumu veya zamanlama mantığının bozulmasını, kimlik doğrulama/otorizasyon süreçlerinin hatalı çalışmasını veya istasyonun yanlış konfigürasyonla kaydedilmesine sebep olur.

## 2. Hedef Varlıklar

Birincil Hedef: CSMS’in BootNotification mesajlarını işleyen WebSocket/JSON ayrıştırma ve kayıt motoru.  
İkincil Hedefler: İstasyon kayıt veritabanı, oturum/connection yöneticisi, zamanlayıcılar (heartbeat), istasyon çevrimiçi/offline karar mantığı ve hizmet sürekliliği.

## 3. İlgili Zafiyetler

- Yetersiz giriş doğrulaması (input validation) ve JSON şema validasyonu.  
- BootNotification alanlarında beklenmeyen uzunluklar veya türler için sınırlandırmaların olmaması (buffer/parse taşmaları).  
- Tekrarlı veya çakışan istasyon kayıtlarını idare edecek tutarlı state yönetiminin eksikliği.  
- Zayıf hata yakalama (exception) ve rate limiting mekanizmaları.  
- TLS/PKI eksik veya zayıf kullanımı sebebiyle oturum sahtekarlığına açık olması.

## 4. Tehdit Kategorisi

STRIDE: Tampering (mesaj manipülasyonu), Denial of Service (hatalı/tekrarlanan BootNotificationlarla kaynak tüketimi, hizmet reddi), Spoofing (sahte CP kimlikleri ile kayıt).

## 5. Saldırı Vektörü ve Adımları

1. Bağlantı Hazırlığı: Saldırgan, hedef CSMS ile bir WebSocket bağlantısı kurar veya mevcut zafiyetli bir CP cihazını ele geçirir.

2. BootNotification Crafting: BootNotification yükünde (payload) beklenmeyen değerler hazırlanır — örn. aşırı uzun vendor stringleri, negatif/float olması gereken int alanlara string gönderme, eksik zorunlu alanlar, veya tarih/zaman alanında geriye/ileri tarihler.

3. Sahteleyerek Gönderme: Tek bir istasyon gibi davranarak veya aynı anda çok sayıda sahte CP ile ardışık/çoğaltılmış BootNotification mesajları gönderilir.

4. Durum Tetikleme: Manipüle edilmiş BootNotification’lar CSMS’de; kayıt çakışması, yanlış heartbeat zamanlaması, duplicate kayıtlar veya hatalı oturum başlatma tetikler.

5. Kaynak Tüketimi ve Hata Zinciri: CSMS ayrıştırıcısı/işleyicisi uzun süreli işlem, exception fırtınası veya bellek sızıntısı ile kaynakları tüketir. Ayrıca uygulama mantığı bozulursa gerçek istasyonların bağlantı/servis kabulü engellenir.

6. İleri Aşamalar (Opsiyonel): Başarılı manipülasyon sonrası saldırgan, oturum mantığındaki açıkları kullanarak yetkisiz komutlar gönderme veya sisteme kalıcı yanlış yapılandırma enjekte etme adımlarına geçebilir.

## 6. Etki Analizi

- Hizmet Sürekliliği: Gerçek istasyonların CSMS ile doğru şekilde oturum açamaması, rezervasyon/başlatma mesajlarının gecikmesi veya reddi.  
- Güvenlik: Sahte istasyonlar nedeniyle faturalama hataları, yetkisiz erişim riski veya yanlış LAL (Local Authorization List) oluşturulması.  
- Operasyonel: Yönetim panellerinde yanlış envanter, artan alarm/uyarı miktarı ve operatör müdahale yükü.  
- Finansal: Kullanılmayan/yanlış faturalandırılan seanslar, hizmet kaybı sebebiyle gelir kaybı ve onarım maliyetleri.

## 7. Tespit Edilebilirlik

- Anormal BootNotification frekans artışı (rate), tekrarlı aynı CP kimlikleri veya kısa aralıkta gelen boot mesajları.  
- Beklenmeyen alan uzunlukları ve JSON parse hataları loglarında artış.  
- CSMS tarafında kayıt/ID çakışmaları ve duplicate entry uyarıları.  
- Heartbeat/connection churn ölçümlerinde istasyon başına oturum açma/kapanma sayısında artış.

## 8. Risk Seviyesi

Yüksek — Bu saldırı, hem hizmet erişilebilirliğini etkileyebilir hem de güvenlik, faturalama ve operasyonel süreçlere zarar verebilir. Özellikle geniş ölçekli veya otomasyon/roaming ortamlarında etkisi kritiktir.

## 9. Önerilen Karşı Önlemler

- Katı JSON şeması validasyonu: BootNotification için zorunlu alanlar, tipler, maksimum uzunluklar ve regex kontrolleri uygulanmalı.  
- Rate limiting & connection throttling: Aynı CP kimliğinden veya IP adresinden gelen BootNotification sıklığı sınırlandırılmalı.  
- Idempotency ve duplicate detection: Aynı istasyon için kısa sürede tekrarlanan boot kayıtları dedupe edilmeli veya inkâr edilmelidir.  
- Güçlü hata izolasyonu: Ayrıştırma/validation hataları asla ana işlem döngüsünü durdurmamalı; hatalar güvenli biçimde yakalanıp loglanmalı.  
- Authentication & Mutual TLS: CS ile CSMS arasında PKI tabanlı karşılıklı kimlik doğrulaması (MTLS) zorunlu hale getirilmeli.  
- Logging & Monitoring: BootNotification anormalliklerini tespit eden SIEM kuralları, alert eşiği ve telemetri toplanmalı.  
- Test & Hardening: Fuzzing/sızma testleri düzenli olarak çalıştırılmalı ve OCPP 2.0 özellikleri mümkün olduğunca kullanılmalı.

## 10. Kaynak

Bu rapor oluşturulurken aşağıdaki kaynaklardan yararlanıldı:  
• Antoun J., Kabir M.E., Moussa B., Atallah R., Assi C., "A Detailed Security Assessment of the EV Charging Ecosystem", IEEE Network, May/June 2020.