D - Denial of Service (Hizmet Reddi)

Hedef: Sistemin (CSMS, istasyon, şebeke) meşru kullanıcılar tarafından erişilemez veya kullanılamaz hale getirilmesi.

1. Saldırı Ağacı - OCPP Flooding (CSMS'e Yönelik)

Hedef: Tüm Şarj Ağını Çevrimdışı Yapmak

Adım 1: Bir Botnet Ağı Kiralamak (veya Güçlü Sunucular Kullanmak)

Adım 2: CSMS OCPP Sunucu Adresini Tespit Etmek
Alt Adım 2a: Bir istasyonun firmware'ini analiz ederek (reverse engineering) IP adresini bulmak.

Adım 3: Sahte İstasyon Bağlantıları Başlatmak
Alt Adım 3a: (mTLS yoksa) Binlerce sahte TCP bağlantısı açarak BootNotification (İstasyon açılış bildirimi) göndermek. CSMS, bu sahte istasyonlar için kaynak (RAM, CPU) ayırır.

Adım 4: Kaynak Tüketme (Flood)
Alt Adım 4a: Bu binlerce sahte bağlantı üzerinden CSMS'e sürekli ve yüksek frekansta Heartbeat veya MeterValues gibi "çöp" OCPP mesajları göndermek.
Sonuç: CSMS sunucusunun bağlantı tablosu, CPU'su veya bant genişliği dolar.

Meşru istasyonların Heartbeat mesajları zaman aşımına uğrar (timeout), CSMS tarafından "çevrimdışı" olarak işaretlenirler ve ağdaki kimse şarj başlatamaz.

2. Sömürü Senaryoları

Şebeke Dengesizliği (Grid Destabilization - En Tehlikelisi): CSMS'i ele geçiren bir saldırgan, bir şehirdeki binlerce istasyona *aynı anda* "Tam Güçte Şarja Başla" (RemoteStartTransaction) komutu gönderir. Bu, yerel elektrik şebekesinde ani ve devasa bir talep artışı yaratarak bölgesel bir elektrik kesintisine (blackout) neden olabilir.

Şarj İstasyonu Kilitlenmesi (Fuzzing): Saldırgan, istasyonun OCPP protokolünü işleyen yazılımına kasıtlı olarak bozuk, hatalı veya beklenmedik formatlarda (fuzzing) binlerce paket gönderir. İstasyonun yazılımı bu hatalı veriyi işleyemez

(örn. buffer overflow), çöker ve yeniden başlatılana kadar hizmet veremez hale gelir.

3. Azaltma Stratejileri (Mitigation)

CSMS Rate Limiting (İstek Sınırı): Her IP adresinden veya istasyondan alınacak saniye başına bağlantı ve mesaj sayısına katı sınırlar (rate limiting) koymak.

Akıllı Şarj (Smart Charging) ve Yük Dengeleme: CSMS'in, şebeke stabilitesini (talep-yanıt sinyalleri) her zaman önceliklendirmesi. Asla tüm istasyonlara aynı anda tam güçte başlama izni vermemesi, şarjları zaman içinde akıllıca dağıtması.

Girdi Doğrulama (Input Validation - Fuzzing Koruması): İstasyon firmware'inin, aldığı tüm OCPP mesajlarının formatını, uzunluğunu ve içeriğini sıkı bir şekilde kontrol etmesi; standart dışı paketleri güvenli bir şekilde reddetmesi.

4. Tespit Mekanizmaları (Detection)

Trafik Anomali Tespiti: CSMS sunucusuna gelen BootNotification veya Heartbeat mesajlarının sayısında (örn. normalin %500 üstünde) ani ve anormal bir artış tespit edildiğinde alarm üretmek.

Kaynak İzleme: CSMS sunucusunun CPU, RAM veya ağ bağlantı sayısının %90'ın üzerine çıkması durumunda alarm üretmek.

Toplu Heartbeat Kaybı: Çok sayıda (örn. 100+) meşru istasyonun aynı anda (örn. 2 dakika içinde) Heartbeat göndermeyi kesmesi durumunda (CSMS'in kilitlendiğini gösterir) alarm üretmek.

D - Denial of Service DREAD Değerlendirmesi

Tehdit Senaryosu: "Şebeke Dengesizliği (Grid Destabilization)"

(CSMS'i ele geçirip tüm istasyonlara aynı anda "Şarja Başla" komutu göndermek.)

D - Damage Potential (Zarar Potansiyeli): 10

Gerekçe: En yüksek potansiyel zarardır. Sadece şarj ağını değil, bölgesel elektrik şebekesini (grid) istikrarsızlaştırabilir. Fiziksel altyapıya (trafolar, vb.) zarar verebilir ve bölgesel elektrik kesintisine (blackout) yol açabilir.

R - Reproducibility (Tekrarlanabilirlik): 7

Gerekçe: Saldırgan CSMS'te admin yetkisini ele geçirdiyse (ki bu zor ykısımdır),

bu toplu komutu göndermesi %100 tekrarlanabilir.

E - Exploitability (İstismar Edilebilirlik): 8
Gerekçe: Bu saldırının kendisi değil, *öncülü* zordur (CSMS'in ele geçirilmesi). Ancak CSMS ele geçirildikten sonra, bu saldırıyı "tetiklemek" çok kolaydır (tek bir API komutu). Bu puan, "CSMS'in ele geçirildiği" varsayımına dayanır.

A - Affected Users (Etkilenen Kullanıcılar): 10
Gerekçe: Sadece EV kullanıcıları değil, o elektrik şebekesine bağlı *tüm* vatandaşlar (hastaneler, evler, trafik ışıkları) etkilenir.

D - Discoverability (Keşfedilebilirlik): 3
Gerekçe: CSMS'i ele geçirme zafiyetini (örn. RCE, kritik BFLA) bulmak zordur. Sistemin şebekeyi etkileme yeteneğini bilmek, derinlemesine sistem bilgisi gerektirir.

Risk Skoru: 38/50 (Kritik Risk)

Sacide Aişenur Direk