E - Elevation of Privilege (Yetki Yükseltme)

Hedef: Düşük yetkili bir hesabın (örn. normal kullanıcı) veya işlemin, sistemdeki bir zafiyetten faydalanarak daha yüksek yetkilere (örn. admin, root) sahip olması.

1. Saldırı Ağacı - API Üzerinden Admin Yetkisi (BFLA)

Hedef: Admin Yetkisi Olmadan İstasyon Fiyatlarını Değiştirmek

Adım 1: Normal Bir Kullanıcı Hesabıyla API'ye Giriş Yapmak
Alt Adım 1a: Mobil uygulamadan giriş yaparak geçerli bir "kullanıcı" oturum anahtarı (JWT token) almak.

Adım 2: Gizli Admin API Endpoint'lerini Keşfetmek
Alt Adım 2a: API dokümantasyonunu veya web sitesi JavaScript dosyalarını inceleyerek POST /api/admin/set-price gibi bir endpoint keşfetmek.

Adım 3: Yetkisiz İstek Göndermek
Alt Adım 3a: Normal "kullanıcı" token'ı ile bu /api/admin/set-price endpoint'ine geçerli bir fiyat listesi JSON'u ile istek göndermek.

Adım 4: Zafiyeti Sömürmek
Alt Adım 4a: API, "403 Forbidden" (Yasak) hatası vermesi gerekirken, "200 OK" (Başarılı) yanıtı döner.

Sonuç: Normal bir kullanıcı, tüm ağın fiyatlandırmasını değiştirme yetkisi kazanmış olur.

2. Sömürü Senaryoları

Arka Uç (Backend) Sistem Ele Geçirme: Admin paneline (örn. SQL Injection ile) veya sunucunun kendisine (örn. SSRF veya RCE ile) erişen saldırgan, CSMS uygulamasından çıkarak sunucunun işletim sisteminde root yetkisine geçer.

Fiziksel Yetki Yükseltme: İstasyonun donanımına fiziksel erişim (UART/JTAG portları) sağlayan saldırgan, önyükleme (bootloader) sürecini kesintiye uğratarak veya belleği manipüle ederek cihazın Linux işletim sisteminde root kabuğu (shell)

elde eder.

Şebeke Kontrolünü Ele Geçirme: (En yüksek seviye). CSMS'te admin yetkisi elde eden saldırgan, CSMS'in bağlı olduğu Tali Dağıtım Merkezi (DSO) veya Akıllı Şebeke (Smart Grid) API'lerine de (eğer varsa) erişim sağlayarak "şebeke kontrol" yetkisine yükselir.

3. Azaltma Stratejileri (Mitigation)

Zorunlu Fonksiyon Seviyesi Yetkilendirme (BFLA Koruması): Her API endpoint'i için (sadece URL değil, her fonksiyon için) "Bu isteği yapan token'daki 'rol' (örn. 'admin') bu işlemi yapmaya yetkili mi?" kontrolünü sunucu tarafında zorunlu kılmak.

Donanım Güvenliği ve Port Koruması: Üretimden sonra JTAG/UART gibi hata ayıklama portlarını fiziksel olarak (veya yazılımsal olarak kalıcı) devre dışı bırakmak. Güvenli Önyükleme (Secure Boot) kullanarak root erişimini engellemek.

En Az Yetki Prensibi (Sistem Seviyesi): CSMS uygulamasının, işletim sisteminde asla root kullanıcısı olarak çalışmaması. Sadece gerekli portlara ve dosyalara erişimi olan kısıtlı bir servis (csms_user gibi) kullanıcısı olarak çalışması.

4. Tespit Mekanizmaları (Detection)

Yetkisiz API Erişimi Alarmı: Bir "kullanıcı" rolünün, /api/admin/ veya /api/internal/ gibi kritik API yollarına erişmeye çalışması durumunda "Kritik" seviyede alarm üretmek ve bu hesabı otomatik olarak kilitlemek.

Rootkit Tespiti: İstasyonun (eğer Linux tabanlıysa), periyodik olarak chkrootkit veya rkhunter gibi araçlarla kendisini tarayarak root seviyesinde bir anomali olup olmadığını CSMS'e raporlaması.

Yetki Değişimi Loglama: CSMS admin panelinde "yeni admin ekleme" veya "kullanıcı rolü değiştirme" gibi eylemlerin özel olarak loglanması ve diğer tüm adminlere bu konuda bir bildirim gönderilmesi.

E - Elevation of Privilege DREAD Değerlendirmesi

Tehdit Senaryosu: "API'de BFLA ile Admin Fonksiyonu Çağırma"

(Normal kullanıcının, api/admin/set-price gibi bir endpoint'i çağırabilmesi.)

D - Damage Potential (Zarar Potansiyeli): 9
Gerekçe: Saldırganın hangi admin fonksiyonunu çağırdığına bağlı olarak (örn. fiyatları sıfırlamak, tüm istasyonları kapatmak) sistemsel kaosa yol açabilir.

R - Reproducibility (Tekrarlanabilirlik): 10
Gerekçe: Zafiyet (API'nin rol kontrolü yapmaması) varsa, %100 tekrarlanabilir.

E - Exploitability (İstismar Edilebilirlik): 4
Gerekçe: İstismar etmesi kolaydır ancak gizli admin endpoint'inin (/set-price) adının bilinmesini gerektirir (Discoverability'ye bağlı).

A - Affected Users (Etkilenen Kullanıcılar): 10
Gerekçe: Yapılan işleme bağlı olarak (fiyat değişikliği, toplu kapatma) ağdaki tüm kullanıcılar ve istasyonlar etkilenir.

D - Discoverability (Keşfedilebilirlik): 5
Gerekçe: Admin endpoint'lerinin adlarını bulmak (örn. JavaScript dosyalarını incelemek, dirb ile taramak) gerekir. IDOR kadar kolay değildir ama imkansız da değildir.

Risk Skoru: 38/50 (Çok Yüksek Risk)

Sacide Aişenur Direk