BELGE BAŞLIĞI: SUNUCU TARAFI İSTEK SAHTECİLİĞİ (SSRF) ZAFİYETİ: ELEKTRİKLİ ARAÇ ŞARJ ALTYAPILARI BAĞLAMINDA ANALİZ VE ÖNLEME YÖNTEMLERİ

BELGE TARİHİ: 2 KASIM 2025

BELGE AMACI: Bu doküman, elektrikli araç (EV) şarj altyapılarını yöneten merkezi sistemler (CSMS) başta olmak üzere, ilgili bilgi sistemlerindeki Sunucu Tarafı İstek Sahteciliği (SSRF) zafiyetini teknik düzeyde analiz etmek, potansiyel risk senaryolarını tanımlamak ve bu zafiyete karşı alınması gereken güvenlik önlemlerini detaylandırmak amacıyla hazırlanmıştır.

1. Giriş

Elektrikli araç şarj ekosistemleri, şarj istasyonları (CS), merkezi yönetim sistemleri (CSMS) ve kullanıcı uygulamalarından oluşan karmaşık ve dağıtık bir yapıya sahiptir. Bu sistemlerin arka planında çalışan yazılımlar ve API'ler, internet üzerinden çeşitli kaynaklarla iletişim kurmak zorundadır. Bu iletişim noktaları, doğru bir şekilde güvenli hale getirilmediğinde, Sunucu Tarafı İstek Sahteciliği (SSRF) gibi kritik zafiyetlere maruz kalabilir.
Bu doküman, SSRF'in EV şarj altyapıları özelindeki risklerini ve bu risklerin bertaraf edilmesi için uygulanması gereken metodolojileri ele almaktadır.

2. Zafiyet Tanımı: Sunucu Tarafı İstek Sahteciliği (SSRF)

Sunucu Tarafı İstek Sahteciliği (OWASP API Security Top 10 - API7:2023), bir saldırganın, zafiyetli bir sunucuyu, sunucunun kendi güvenlik bağlamından (kendi iç ağından veya kendi üzerinden) başka bir sunucuya istenmeyen bir ağ isteği yapmaya zorlamasıdır.
Zafiyetin temel çalışma prensibi şu şekildedir:

- Uygulama, bir fonksiyonu yerine getirmek için kullanıcıdan bir URL veya IP adresi gibi bir girdi alır.
- Sunucu, bu girdiyi yeterince doğrulamadan veya filtrelemeden, bu hedefe bir ağ isteği (örn. HTTP GET) yapar.
- Saldırgan, bu girdi alanını manipüle ederek sunucunun normalde

erişmemesi gereken hedeflere (örn. iç ağdaki cihazlar, sunucunun kendisi) istek göndermesini sağlar.

Bu saldırının en tehlikeli yönü, saldırganın güvenlik duvarını (firewall) içeriden aşmasını sağlamasıdır. İstek, dışarıdan (saldırgandan) değil, içerideki "güvenilir" sunucudan geldiği için, iç ağ güvenlik mekanizmaları bu isteğe izin verebilir.

3. EV Şarj Altyapıları (CSMS) Bağlamında Risk Senaryoları

SSRF zafiyeti, genellikle CSMS platformlarının web arayüzlerinde veya API'lerinde bulunan ve dış kaynaklara erişim gerektiren fonksiyonlarda ortaya çıkar.

Senaryo 1: İstasyon Sağlık Kontrolü (Health Check) Fonksiyonu

Birçok CSMS, operatörlerin bir istasyonun IP adresini veya alan adını girerek o istasyonun çevrimiçi olup olmadığını kontrol etmesine olanak tanır.

- Zafiyetli Özellik: POST /api/v1/diagnostics/check_status
- Zafiyetli Parametre: {"url": "http://istasyon-ip-adresi.com/status"}
- Saldırı: Saldırgan, bu parametreyi değiştirerek iç ağı tarayabilir:
- {"url": "http://192.168.1.1"} (İç ağdaki router veya sunucu)
- {"url": "http://10.0.0.50:5432"} (İç ağdaki PostgreSQL veritabanı portu)
- {"url": "http://localhost:8080/admin-panel"} (CSMS sunucusunun kendi üzerindeki yönetim paneli)

Senaryo 2: Dış Kaynaktan Firmware veya Konfigürasyon Yükleme

CSMS, istasyonlara yeni firmware yüklemek için bir URL parametresi alabilir.

- Zafiyetli Özellik: POST /api/v1/firmware/download_from_url
- Zafiyetli Parametre: {"source_url": "http://firmware-sunucusu.com/v1.2.zip"}
- Saldırı: Saldırgan, bu özelliği kullanarak sunucunun yerel dosyalarını okumaya çalışabilir:
- {"source_url": "file:///etc/passwd"} (Sunucudaki kullanıcı listesi)
- {"source_url": "file:///opt/csms/config/db.ini"} (Veritabanı bağlantı bilgileri)

Senaryo 3: Bulut Altyapısı Meta-Veri Servisine Erişim

Modern CSMS platformları sıklıkla AWS, Azure veya Google Cloud gibi bulut altyapılarında barındırılır. Bu platformlar, çalışan sunuculara 169.254.169.254 gibi özel bir IP adresi üzerinden geçici kimlik bilgileri (erişim anahtarları) sağlar.

- Saldırı: Saldırgan, herhangi bir zafiyetli URL parametresine bu adresi hedefler:
- {"url": "http://169.254.169.254/latest/meta-data/iam/security-credentials/"}

- Etkisi: Sunucu, kendi meta-veri servisine bu isteği yapar ve dönen yanıtı (tüm bulut altyapısını yönetme yetkisine sahip olabilecek erişim anahtarları) saldırgana sızdırabilir. Bu, felaketle sonuçlanabilecek bir senaryodur.

4. Potansiyel Etkiler

Başarılı bir SSRF saldırısının sonuçları şunları içerebilir:

- İç Ağın Haritalandırılması: Güvenlik duvarının arkasındaki sunucuların, veritabanlarının ve servislerin keşfedilmesi.
- Kritik Veri Sızıntısı: Veritabanı bağlantı dizeleri, API anahtarları, kullanıcı verileri ve sistem yapılandırma dosyalarının çalınması.
- Altyapı Kimlik Bilgilerinin Çalınması: Özellikle bulut ortamlarında, tüm altyapıyı tehlikeye atacak yönetici anahtarlarının ele geçirilmesi.
- İç Servislere Yetkisiz Erişim: Dışarıya kapalı olan ve kimlik doğrulama mekanizması zayıf olan iç yönetim panellerine (örn. veritabanı yönetim arayüzleri, dahili API'ler) erişim.
- Hizmet Reddi (DoS): Sunucunun kendisine veya diğer kritik iç servislere sürekli istekler gönderilerek kaynakların tüketilmesi.

5. Önleme Yöntemleri ve Güvenlik Stratejileri

SSRF zafiyetini önlemek için katmanlı bir savunma stratejisi uygulanmalıdır.

5.1. Girdi Doğrulama: Beyaz Liste (Allow List) Yaklaşımı

En etkili savunma yöntemidir. Kullanıcıdan alınan girdinin, önceden tanımlanmış, güvenli ve kısıtlı bir adres listesiyle (beyaz liste) tam olarak eşleşmesi zorunlu tutulmalıdır.

- Örnek: Eğer fonksiyon sadece belirli firmware sunucularından veri çekecekse, sadece o alan adlarına (örn. firmware.operator.com) izin verilmelidir.
- Uzak Durulması Gereken Yöntem: Kara liste (block list) yaklaşımı (örn. localhost, 127.0.0.1 gibi adresleri engellemek) yetersizdir. Saldırganlar bu listeleri [::1] (IPv6), 127.0.0.1.nip.io (DNS hileleri) veya URL kodlama gibi tekniklerle kolayca aşabilir.

5.2. Ağ Seviyesinde Kısıtlama

Uygulama sunucusunun ağ erişimi "en az yetki prensibine" göre kısıtlanmalıdır.

- Egress (Dışa Giden) Kuralları: CSMS sunucusunun, iç ağdaki veritabanı sunucularına veya diğer yönetim arayüzlerine HTTP/HTTPS isteği yapması güvenlik duvarı (firewall) seviyesinde engellenmelidir.

- Segmentasyon: Uygulama sunucuları, kritik veritabanları ve yönetim servisleri farklı ağ segmentlerinde bulunmalıdır.

5.3. Yanıt İşleme

Hedef sunucudan dönen yanıtın tamamı asla doğrudan kullanıcıya (saldırgana) döndürülmemelidir.

- Uygulama, sadece ihtiyaç duyduğu bilgiyi (örn. "Bağlantı başarılı" mesajı veya bir HTTP durum kodu) işlemeli ve kullanıcıya genel bir durum bilgisi sunmalıdır.
- Bu, saldırganın iç ağ taraması yaparken aldığı detaylı hata mesajlarını veya banner bilgilerini görmesini engeller.

5.4. Protokol Kısıtlaması

Eğer özellik sadece HTTP/HTTPS gerektiriyorsa, file:///, ftp://, gopher:// gibi diğer protokoller URL ayrıştırıcı seviyesinde engellenmelidir.

6. Sonuç

Sunucu Tarafı İstek Sahteciliği (SSRF), elektrikli araç şarj istasyonlarını yöneten merkezi sistemler (CSMS) için ciddi bir tehdittir. Saldırganların, güvenilir sunucular üzerinden iç ağlara sızmasına ve kritik verilere erişmesine olanak tanır. Bu riskin yönetimi, yalnızca girdi filtrelemeye dayalı olmamalı; sıkı bir beyaz liste (allow list) politikası, ağ segmentasyonu ve güvenli kodlama (SSDLC) pratiklerini içeren çok katmanlı bir güvenlik yaklaşımını gerektirmektedir.

Sacide Aişenur Direk