## BÖLÜM 1: Saldırı Senaryosu Metni

### Teşhis (Diagnostics) Fonksiyonlarının Kötüye Kullanılmasıyla Hassas Konfigürasyon Verilerinin Sızdırılması

**1. Senaryonun Amacı** Bakım ve sorun giderme amacıyla tasarlanmış olan OCPP teşhis fonksiyonlarını (GetDiagnostics, TriggerMessage) istismar ederek, normalde erişilememesi gereken hassas sistem bilgilerini, log dosyalarını, ağ yapılandırmasını ve hata depolanmış şifreleri sızdırmak.

**2. Senaryo Özeti** Saldırgan, CSMS'i taklit ederek veya meşru bir CSMS operatör hesabını ele geçirerek hedef CP'ye bir GetDiagnostics isteği gönderir. Bu istek, CP'nin teşhis loglarını belirtilen bir FTP(S) veya HTTP(S) sunucusuna yüklemesini tetikler. Saldırgan, bu sunucu adresini kendi kontrolündeki bir sunucu olarak belirler. Eğer CP'nin teşhis dosyaları yeterince temizlenmemişse (sanitized), bu dosyalar içerisinde Wi-Fi şifreleri, ağ geçidi adresleri, CSMS kimlik bilgileri veya diğer istasyonların IP adresleri gibi kritik bilgiler bulunabilir.

**3. Hedef Varlıklar** ● Birincil: CP'nin loglama ve teşhis mekanizması. ● İkincil: CP'de depolanan tüm sistem logları, yapılandırma dosyaları ve geçici veriler.

**4. İlişkili Tehditler (STRIDE)** ● Bilgi İfşası (Information Disclosure): Hassas sistem ve ağ bilgileri yetkisiz bir tarafa sızdırılır. ● Sahtekarlık (Spoofing): Saldırı, genellikle sahte bir CSMS isteği ile başlatılır. ● Yetki Yükseltme (Elevation of Privilege): Sızdırılan bilgiler (örn. root şifresi), saldırganın daha sonra CP üzerinde tam kontrol sağlaması için kullanılabilir.

**5. Saldırıda Faydalanılan Zafiyetler** ● Teşhis dosyalarının yüklenmeden önce hassas bilgileri (şifreler, anahtarlar, PII) temizleyen (sanitization/redaction) bir süreçten geçmemesi. ● GetDiagnostics komutunun, herhangi bir ek yetkilendirme veya onay olmaksızın, sadece standart CSMS yetkisiyle çalıştırılabilmesi. ● CP'nin, teşhis dosyalarını yükleyeceği sunucunun (URL) güvenilirliğini veya sahipliğini doğrulamaması. ● Güvensiz dosya aktarım protokollerinin (FTP gibi) kullanılmasına izin verilmesi, verilerin transit sırasında çalınmasına olanak tanır.

**6. Saldırı Adımları (Adım Adım Simülasyon)** ● Adım 1 (Sızma): Saldırgan, bir oltalama (phishing) saldırısı ile bir CSMS operatörünün kimlik bilgilerini çalar veya ağda bir MitM pozisyonu elde eder. ● Adım 2 (Sunucu Hazırlığı): Saldırgan, internet üzerinde bir FTP sunucusu kurar ve log dosyalarını beklemeye başlar. ● Adım 3 (Komut Gönderme): Saldırgan, ele geçirdiği CSMS hesabını kullanarak veya sahte bir mesaj oluşturarak hedef CP'ye bir GetDiagnostics.req mesajı gönderir. Mesajın location parametresi, saldırganın FTP sunucusunun adresini (ftp://attacker.com/logs/) içerir. ● Adım 4 (Veri Yükleme): CP, komutu alır ve dahili loglarını, yapılandırma dökümlerini ve sistem durumu dosyalarını bir arşiv dosyası (.zip veya .tar.gz) haline getirir. Ardından bu arşivi, belirtilen FTP adresine yükler. ● Adım 5 (Analiz): Saldırgan, FTP sunucusuna gelen arşiv dosyasını indirir ve içeriğini analiz eder. Dosyaların içinde, /etc/wpa_supplicant.conf dosyasından sızan Wi-Fi şifreleri, OCPP yapılandırma dosyasından sızan BasicAuthPassword veya diğer CP'lerin IP adreslerini bulabilir. ● Adım 6 (Genişleme): Saldırgan, elde ettiği bu yeni bilgileri kullanarak ağdaki diğer cihazlara (diğer CP'ler, yerel ağdaki diğer sistemler) saldırmak veya CP üzerinde kalıcı bir erişim sağlamak için kullanır.

**7. Olası Sonuçlar ve Etkiler** ● Geniş Kapsamlı Ağ Sızıntısı: Sadece tek bir CP değil, tüm yerel şarj ağının topolojisi ve güvenlik bilgileri açığa çıkabilir. ● Zincirleme Saldırılar: Elde edilen kimlik bilgileri, tüm şarj istasyonu filosuna yönelik daha büyük bir saldırının başlangıç noktası olabilir. ● Yasal ve Uyumluluk Sorunları: GDPR gibi veri koruma yönetmelikleri kapsamında, kişisel verilerin veya hassas bilgilerin sızdırılması ciddi para cezalarına yol açabilir.

**8. Tespit Yöntemleri (Detection)** ● URL Beyaz Listesi (Whitelisting): CP'ler, yalnızca önceden tanımlanmış, güvenilir sunucu adreslerine (whitelist) teşhis dosyası yüklemelidir. Bilinmeyen bir URL'ye yapılan yükleme girişimi engellenmeli ve loglanmalıdır. ● Ağ Çıkış Filtrelemesi (Egress Filtering): Kurumsal güvenlik duvarı, CP'lerden internet üzerindeki bilinmeyen veya şüpheli FTP sunucularına giden bağlantıları engellemelidir. ● Komut İzleme: GetDiagnostics komutlarının kullanım sıklığı ve hedef URL'leri CSMS tarafından izlenmelidir. Bir operatörün kısa sürede çok sayıda istasyondan teşhis istemesi veya bilinmeyen bir URL kullanması şüpheli bir aktivitedir.

**9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)** ● Veri Temizleme (Data Sanitization): CP yazılımı, teşhis dosyalarını yüklemeden önce, içindeki tüm şifreleri, özel anahtarları, IP adreslerini ve diğer hassas bilgileri otomatik olarak sansürleyen veya kaldıran bir modüle sahip olmalıdır. ● Güvenli Protokoller: FileTransferProtocols yapılandırma değişkeni, sadece FTPS veya HTTPS gibi güvenli ve şifreli protokolleri içerecek şekilde ayarlanmalıdır. FTP gibi güvensiz protokollere izin verilmemelidir. ● Ayrıcalıklı İşlem Onayı: GetDiagnostics gibi potansiyel olarak tehlikeli bir komutun çalıştırılması, CSMS arayüzünde ikinci bir onay adımı veya farklı bir yetkili tarafından doğrulama gerektirmelidir. ● Güvenli Geliştirme Yaşam Döngüsü (SSDLC): Geliştiriciler, loglara asla hassas bilgileri düz metin olarak yazmamaları konusunda eğitilmeli ve kod analiz araçları bu tür sızıntıları tespit etmek için kullanılmalıdır.

---

## BÖLÜM 2: Senaryonun SWOT Analizi

**Senaryonun SWOT Analizi (Saldırgan Perspektifi)**

Bu analiz, saldırıyı gerçekleştiren tarafın bu yöntemi kullanmasının avantajlarını (Güçlü Yönler), dezavantajlarını (Zayıf Yönler), bu saldırıdan doğan potansiyel fırsatları (Fırsatlar) ve saldırının başarısını engelleyebilecek riskleri (Tehditler) ele alır.

---

### GÜÇLÜ YÖNLER (Strengths)

*Saldırının doğasında olan ve onu etkili kılan avantajlar:*

- **Meşru Fonksiyon Kullanımı:** Saldırı, sistemin normal bakımı için tasarlanmış standart bir OCPP fonksiyonu (`GetDiagnostics`) kullanarak gerçekleştirilir. Bu, saldırı trafiğinin normal operasyonel trafik arasında gizlenmesini kolaylaştırır.
- **Yüksek Değerli Veri Potansiyeli:** Başarılı bir saldırı, Wi-Fi şifreleri, CSMS kimlik bilgileri, ağ topolojisi ve hatta root şifreleri gibi son derece kritik ve değerli verileri tek seferde sızdırabilir.

- **Basit Komut Yapısı:** İlk erişim sağlandıktan sonra (Adım 1), saldırının kendisi (Adım 3) teknik olarak basittir; saldırganın hedef adresi içeren tek bir `GetDiagnostics.req` mesajı göndermesi yeterlidir.
- **Asenkron ve Pasif Veri Toplama:** Saldırgan komutu gönderdikten sonra aktif olarak sistemde kalmak zorunda değildir. CP (Şarj Noktası), tüm işi kendisi yapar (veri toplama, sıkıştırma, yükleme) ve veriyi doğrudan saldırganın sunucusuna "teslim eder".
- **Düşük Yetki Gereksinimi:** Senaryoda belirtildiği gibi, bu komut genellikle standart CSMS operatör yetkisiyle çalışır ve ek, yükseltilmiş bir yetki veya onay (ikinci bir faktör) gerektirmez.

---

**ZAYIF YÖNLER (Weaknesses)**

*Saldırganın bu yöntemi kullanırken karşılaştığı zorluklar veya kısıtlamalar:*

- **Ön Koşul Gereksinimi:** Bu saldırı, tek başına birincil giriş vektörü değildir. Saldırganın **öncelikle** bir CSMS operatör hesabını (örn. oltalama ile) ele geçirmesi veya ağda bir Man-in-the-Middle (MitM) pozisyonu elde etmesi gerekir (Adım 1).
- **"Veri Temizleme" (Sanitization) Bağımlılığı:** Saldırının tüm başarısı, hedef CP yazılımının log dosyalarını yüklemeden önce *temizlememesine* (sanitization) bağlıdır. Eğer CP, şifreleri ve anahtarları sansürlüyorsa, saldırganın eline hiçbir değerli veri geçmez.
- **Garantisiz Sonuç:** Log dosyaları elde edilse bile, bu dosyaların o an için değerli bilgiler (örn. "root şifresi") içereceğinin bir garantisi yoktur. Saldırganın, değerli bir bilgi kırıntısı bulmak için potansiyel olarak çok büyük log dosyalarını analiz etmesi gerekebilir.
- **Sunucu Kurulum İhtiyacı:** Saldırganın logları alabilmesi için internete açık, erişilebilir bir FTP(S) veya HTTP(S) sunucusu kurması ve yapılandırması gerekir (Adım 2).

---

**FIRSATLAR (Opportunities)**

*Saldırının başarılı olması durumunda saldırgana sağladığı ek avantajlar ve genişleme yolları:*

- **Zincirleme Saldırılar (Yatay Genişleme):** En büyük fırsattır. Sızdırılan Wi-Fi şifreleri veya ağ bilgileri, saldırganın sadece o CP'ye değil, aynı yerel ağdaki (LAN) diğer şarj istasyonlarına veya diğer kurumsal sistemlere sızmasını sağlar (Adım 6).
- **Yetki Yükseltme (Dikey Genişleme):** Sızdırılan bir CSMS `BasicAuthPassword` veya cihazın `root` şifresi, saldırgana o cihaz veya hatta tüm CSMS üzerinde tam kontrol (admin/root erişimi) sağlayabilir.
- **Tüm Filoyu Hedef Alma:** Bir CSMS hesabı üzerinden elde edilen bilgiler veya kimlik bilgileri, aynı CSMS'e bağlı *tüm şarj istasyonu filosuna* yönelik daha geniş kapsamlı bir saldırı başlatmak için kullanılabilir.
- **Sektörel Zafiyet:** Metinde de belirtildiği gibi, bu tür zafiyetlerin (loglara hassas veri yazma, FTP gibi güvensiz protokolleri destekleme) sektörde yaygın olması, bu saldırı

senaryosunun *farklı üreticilerin birçok cihazına* karşı tekrar tekrar kullanılabilme fırsatını doğurur.

---

**TEHDİTLER (Threats)**

*Saldırganın başarısını doğrudan tehdit eden veya saldırının tespit edilmesine yol açan savunma mekanizmaları:*

- **URL Beyaz Listesi (Whitelisting):** En büyük tehdittir. Eğer CP, log dosyalarını *sadece* önceden tanımlanmış güvenilir sunucu (örn. `diagnostics.uretim.com`) adreslerine gönderecek şekilde yapılandırılmışsa, saldırganın `ftp://attacker.com` adresine yaptığı istek doğrudan engellenir ve alarm üretir.
- **Ağ Çıkış Filtrelemesi (Egress Filtering):** Kurumsal güvenlik duvarı (firewall), CP'lerin içeriden dışarıya, özellikle bilinmeyen IP adreslerine veya güvensiz FTP portlarına (Port 21) giden bağlantılarını engellerse, CP log dosyasını yükleyemez.
- **Anomali Tespiti ve Komut İzleme:** CSMS tarafında, bir operatörün normal dışı bir şekilde (`GetDiagnostics` komutunu sık kullanması, bilinmeyen bir URL kullanması vb.) hareket etmesinin izlenmesi, saldırının (veya ele geçirilmiş hesabın) hızla tespit edilmesini sağlayabilir.
- **Güvenli Protokol Zorlaması:** CP'nin *sadece* FTPS veya HTTPS gibi şifreli protokolleri kullanmaya zorlanması ve güvensiz FTP'ye izin vermemesi (saldırganın işini zorlaştırır) veya
- **Veri Temizleme (Data Sanitization):** CP yazılımının logları yüklemeden önce *otomatik olarak sansürlemesi*, saldırıyı tamamen etkisiz hale getiren birincil önlemdir.

**Sanal Ortamda Test İçin Referans Makaleler** ● Alcaraz, C., Cumplido, J., & Triviño, A. (2023). "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0." ● INL (Idaho National Laboratory) Raporları (örn. "Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment")