

IEC 61851 İletişim Kesintisi – Enerji Akışı Devam Ediyor (Protokol Uyum Anomalisi)

1. Anomali Tanımı

Anomali Tanımı — “Loglarda Açık Metin Kimlik/Jeton (Credential) Sızıntısı”

EVSE, CSMS ve ilgili servislerin loglarında kullanıcı kimlikleri (ör. idTag, RFID UID), yetkilendirme jetonları (API key, session ID) veya temel kimlik bilgileri (kullanıcı adı, parola, BasicAuth) açık metin olarak tutulmaktadır.

Bu durum, kimlik bilgilerinin loglara erişen biri tarafından ele geçirilmesine neden olabilir. Böyle bir durumda saldırgan yetkisiz oturum başlatabilir veya sistemleri zincirleme ele geçirebilir. Ayrıca olay, **KVKK / GDPR** kapsamında ciddi gizlilik ihlalidir.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama
Yazılım	Hatalı loglama yöntemi	Geliştirici hassas verileri hariç tutmamış veya maskeleme fonksiyonu devre dışı bırakılmış.
Yazılım	Yetersiz kimlik yönetimi	Token veya kullanıcı bilgileri debug seviyesinde loglanıyor.
Donanım	Güvenli depolama eksikliği	Log dosyaları korumasız sürücülerde tutuluyor, şifrelenmemiş disklerde erişime açık.
Protokol	Güvensiz kimlik doğrulama	BasicAuth veya düz metin kimlik bilgileri kullanıldığı için logda açık görünüyor.
İletişim	Merkezi loglama maskeleme hatası	SIEM veya log toplayıcıda maskeleme kuralı uygulanmadığından tüm içerik açık şekilde kaydediliyor.

3. Olası Riskler ve Etkiler

- **Bilgi Sızıntısı:** Kullanıcı kimliklerinin veya token’ların ifşası, yetkisiz erişim ve hesap devralma riski doğurur.
- **Zincirleme Saldırı Riski:** Elde edilen oturum jetonlarıyla diğer sistemlere sıçrama (lateral movement) mümkün hale gelir.
- **Mevzuat Riski:** Kişisel verilerin maskesiz tutulması, **KVKK / GDPR** ihlali anlamına gelir; para cezası ve güven kaybı riski taşır.

4. İlgili Standart Referansı

- **ISO/IEC 27001 – Bilgi Güvenliği Yönetim Sistemi**
 - Madde A.12.4: Log kayıtlarında gizli bilgilerin maskeleme / anonimleştirme gerekliliği.
- **OWASP Logging Cheat Sheet**

5. Çözüm Önerileri

Yazılım Düzeyinde:

- Tüm loglama fonksiyonlarında **masking / redaction** (ör. `user_id=****`) zorunlu hale getirilmelidir.
- Hata ayıklama (debug) logları üretim ortamında devre dışı bırakılmalıdır.

Protokol Düzeyinde:

- Kimlik doğrulama işlemleri **TLS 1.3** üzerinden yapılmalı; BasicAuth yerine **token tabanlı kimlik doğrulama** kullanılmalıdır.

İletişim ve Loglama Düzeyinde:

- Merkezi log toplayıcıda maskeleyme kuralı (ör. regex tabanlı redaction) aktif edilmelidir.
- Loglar şifreli depolarda tutulmalı ve erişim sadece yetkili rollere verilmelidir.

6. Sonuç ve Değerlendirme

Bu anomali, bilgi güvenliği açısından **kritik** seviyededir.

Açık metin kimlik bilgileri, saldırganların sistemin tamamına erişebilmesine olanak tanıyabilir.

Dolayısıyla olay, “**Yüksek Öncelikli Gizlilik İhlali (Confidentiality Breach)**” olarak sınıflandırılmalı ve yazılım sürüm kontrolü, log yönetimi ve erişim politikaları kapsamında düzenli denetlenmelidir.