SWOT Analizi: OCPP Komut Anomalisi

GÜÇLÜ YÖNLER (Strengths)

- Dijital imza kontrolü sayesinde yetkisiz OCPP mesajları kolayca tespit edilebilir.
- Olay logları güvenlik sistemine iletildiğinden olay sonrası analiz mümkündür.
- OCPP protokolünün standart yapısı, anomali tespiti için sistematik denetimlerin uygulanmasını kolaylaştırır.
- Mutual TLS (karşılıklı sertifika) ve nonce tabanlı kimlik doğrulama ile güvenlik artırılabilir.
- CSMS-istemci iletişimi saydam olduğu için manipüle edilmiş komutların kaynağı daha kolay belirlenebilir.

ZAYIF YÖNLER (Weaknesses)

- Zayıf TLS konfigürasyonu veya eksik kimlik doğrulama sistemleri MITM saldırı riskini artırır.
- Komut mesajlarının imzalanmaması, sahte RemoteStart veya RemoteStop mesajlarının kabul edilmesine yol açabilir.
- Gerçek zamanlı imza doğrulama sistemin performansında gecikmeye neden olabilir.
- Protokolün açık yapısı, siber saldırganların çalışma mantığını öğrenmesini kolaylaştırır.
- Eski istasyonlar, yeni güvenlik yamalarıyla uyumlu olmayabilir.

FIRSATLAR (Opportunities)

- Yapay zekâ tabanlı anomali tespiti sistemleriyle erken uyarı mekanizmaları geliştirilebilir.
- Endüstri 4.0 ve akıllı enerji sistemleriyle entegrasyon, güvenli OCPP iletişimine olan talebi artırır.
- Bu anomali türü, siber güvenlik eğitimlerinde örnek vaka olarak kullanılabilir.
- Yeni nesil OCPP sürümleri için güvenlik standartlarının geliştirilmesine katkı sağlar.
- ISO 15118 ve IEC 61851 gibi standartlarla uyumluluk, sistemin pazar değerini yükseltebilir.

TEHDİTLER (Threats)

- Kimliği doğrulanmamış uzak komutlar enerji akışını kesintiye uğratarak maddi zarara neden olabilir.
- MITM ve spoofing saldırıları veri manipülasyonu veya yetkisiz erişime yol açabilir.
- Yeni saldırı türleri mevcut güvenlik kontrollerini atlatabilir.

- Log kayıtlarının değiştirilmesi veya silinmesi, olay tespitini geciktirir.
- Zincirleme etkiyle bir istasyondaki anomali, diğer bağlı sistemleri etkileyebilir.

GENEL DEĞERLENDİRME

OCPP Komut Anomalisi, elektrikli araç şarj altyapısında ciddi güvenlik riskleri oluşturur.
Ancak dijital imza kontrolü, mutual TLS ve gelişmiş log analizleri ile bu riskler azaltılabilir.
Uzun vadede bu tür anomalilerin incelenmesi, daha güvenli protokol tasarımlarının gelişmesine katkı sağlar.