ANOMALI RAPORU

Fail-Open Davranisi - Auth Servis Kapali

1. Anomali Tanimi

Sistem, kimlik dogrulama servisi (Auth Servis / CSMS) erisilemez hale geldiginde fail-open davranisi gostermektedir. Bu durum, fail-closed prensibini ihlal eder. Sonuc olarak, bir saldirgan Hizmet Reddi (DoS) saldirisi ile Auth Servis'i devre disi birakabilir ve istasyonu yetkisiz olarak kullanabilir.

2. Kapsam

Bilesen: EVSE - CSMS Iletisimi (OCPP / Auth Flow)
Fonksiyon: Kimlik dogrulama ve sarj baslatma kontrolu
Kapsam: Tum cevrimdisi senaryolari etkiler.

3. Senaryo (Adim Adim)

1. Normal Durum	EVSE, Auth Servis'e kimlik dogrulama istegi gonderir. Eger yanit OK ise, sarj baslar.
2. Ariza Durumu	Auth Servis, DoS saldirisi nedeniyle erisilemez hale gelir.
3. Istasyon Karari	Fail-open politikasindan dolayi EVSE, yanit beklemeden sarj islemini baslatir.
4. Sonuc	Yetkisiz enerji kullanimi, log kaydi yok, gelir kaybi.

4. Etkiler ve Riskler

Finansal	Ucretsiz sarj islemleri nedeniyle dogrudan gelir kaybi.
Operasyonel	Sunucu arizasinda sistem guvenli modda kalamaz.
Guvenlik	Kimlik dogrulama atlanir ve yetkisiz kullanim olur.
Itibar	Sistemin kotuye kullanilmasi guven kaybina neden olur.

5. Kok Neden Analizi

Sistem tasariminda hizmet surekliligi guvenligin onune konmustur. Auth modulu icin cevrimdisi yedek politika eksik veya hatalidir. Fail-closed davranisi dogru sekilde uygulanmamis veya test edilmemistir.

6. Tespit ve Dogrulama

Auth Servis erisilemez hale getirildiginde EVSE, kimlik dogrulama olmadan sarj islemini baslatmistir. Beklenen: Fail-Closed. Gercek: Fail-Open. Zafiyet dogrulandi.

7. Onerilen Duzeltici Aksiyonlar

1. Sistem mantigi fail-closed davranisina gecmelidir.
2. Sadece belirli kullanicilar icin cevrimdisi cache veya whitelist uygulanmalidir.
3. DoS dayanikliligi load balancer ve rate limitlerle guclendirilmelidir.
4. Fail-open durumlari icin loglama ve alarm mekanizmasi eklenmelidir.

8. Siniflandirma

CWE-703: Improper Handling of Exceptional Conditions
CWE-287: Improper Authentication
OWASP A07-2021: Identification and Authentication Failures

9. Risk Seviyesi

Olasilik	Yuksek

Etki	Kritik
Risk Puani	9.2 / 10 — Kritik

10. Sonuc

Fail-open davranisi, mimari acidan kritik bir zayifliktir. Enerji, odeme veya kimlik dogrulama yapan sistemler, guvenligi saglamak ve kotuye kullanimi onlemek icin her zaman fail-closed prensibini uygulamalidir.

Kaynakca

[1] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., & Lloret, J. (2023). Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. Sensors, 23(15), 6716. https://doi.org/10.3390/s23156716

[2] Ganesan, S., Patel, D. K., & Chokalingam, R. (2024). Security of Electric Vehicle Charging Stations. Journal of Electrical and Computer Engineering Research, 4(4).*

[3] Tanyildiz, H. et al. (2025). Detection of cyber attacks in electric vehicle charging station supply equipment. Scientific Reports.

[4] Mitikiri, S. B. (2025). Cyber–physical security in EV charging infrastructure. Journal of Energy Systems Engineering, Elsevier.

[5] Kaur, A. (2023). Cybersecurity Challenges in the EV Charging Ecosystem. ACM Digital Library.