CAN Bus Mesaj Şifreleme Eksikliği – Sniffing Yoluyla Bilgi Sızması (Protokol Güvenlik Açığı)

---

1. Anomali Tanımı

CAN Bus (Controller Area Network), araç içerisindeki elektronik kontrol üniteleri (ECU'lar) arasında iletişimi sağlar. Ancak bu protokolde gönderilen mesajlar **şifrelenmeden**, yani **açık metin (plaintext)** olarak iletilmektedir.
Bu durum, CAN hattına fiziksel erişimi olan bir aktörün, özel bir donanım yardımıyla bu trafiği **dinlemesine (sniffing)** ve hassas bilgileri elde etmesine olanak tanır.

Açıklanan bu anomali, özellikle **gizlilik ve ileri saldırılar** açısından ciddi güvenlik zafiyetleri doğurur.

2.Olası Nedenler

Kategori	Olası Sebep	Açıklama
Protokol	Şifreleme standardı eksikliği	CAN Bus protokolü doğal olarak veri şifrelemesi içermez.
Donanım	Fiziksel portlara erişim	OBD-II gibi portlar üzerinden CAN hattına doğrudan bağlantı yapılabiliyor.
Yazılım	Güvenli mimari eksikliği	ECU yazılımları, mesaj gizliliği veya kimlik doğrulama kontrolleri uygulamıyor.

3. Olası Riskler ve Etkiler

- **Veri Gizliliği İhlali**: Araç içi sistemlerin durumu (frenleme, hız, yönlendirme vb.) kötü niyetli kişilerce izlenebilir.
- **Hazırlık Aşaması**: Sniffing ile elde edilen bilgiler, spoofing (mesaj taklidi) veya DoS saldırıları için kullanılabilir.
- **Yasal Riskler**: Kişisel verilerin (konum, hız, davranış kalıpları) açık şekilde iletilmesi, GDPR gibi veri koruma yasalarına aykırıdır.

4. İlgili Standart Referansı

ISO 26262 – Road Vehicles – Functional Safety
SAE J1939 – CAN-based Protocol for Heavy-Duty Vehicles
ISO 11898 – Road Vehicles – Controller Area Network (CAN)

Donanım Düzeyinde:

5. Çözüm Önerileri

Donanım Düzeyinde:

- Veri hattına erişimi engelleyen fiziksel izolasyon veya firewall uygulanmalıdır.

- OBD-II portuna özel erişim kontrol mekanizmaları (örneğin PIN veya token tabanlı yetkilendirme) entegre edilmelidir.

Yazılım Düzeyinde:

- ECUs arası veri alışverişi, uygulama katmanında şifreleme (AES, ECC vb.) ile güvence altına alınmalıdır.
- Mesajlara dijital imza veya mesaj doğrulama kodları (MAC) eklenmelidir.

Test Aşamasında:

- CAN hattı üzerinden sniffing ve replay testleri yapılmalıdır.
- Araç yazılımında "güvenli mesajlaşma" politikalarının etkinliği doğrulanmalıdır.

6. Sonuç ve Değerlendirme

CAN Bus üzerindeki mesajların şifrelenmemesi, özellikle modern bağlantılı araç mimarilerinde ciddi bir güvenlik açığı teşkil etmektedir.
Bu açık, gizli bilgi sızdırılması, sürücü davranışlarının izlenmesi ve saldırılara zemin hazırlanması gibi riskleri barındırır.

Dolayısıyla bu durum, **"kritik güvenlik açığı"** olarak değerlendirilmelidir ve hem donanım hem yazılım düzeyinde protokol üstü önlemlerle giderilmelidir.

---

7. Kaynakça

- O.A.M. Al Isawi, "Electric Vehicles CAN Bus Cyber-Attacks Detection," Khalifa University, 2023. PDF
- ISO 11898 – Road Vehicles – Controller Area Network
- ISO 26262 – Functional Safety for Automotive
- Miller & Valasek, "A Survey of Remote Automotive Attack Surfaces," 2014.
- SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

7.Kaynakça

1. IEC 61851-1:2017 – *Electric Vehicle Conductive Charging System – Part 1: General Requirements*, International Electrotechnical Commission (IEC), Geneva, Switzerland.
2. ISO 15118-2:2014 – *Road Vehicles – Vehicle to Grid Communication Interface – Part 2: Network and Application Protocol Requirements*, International Organization for Standardization.
3. UL 2202:2019 – *Standard for Electric Vehicle (EV) Charging System Equipment*, Underwriters Laboratories Inc.
4. IEEE 2030.1.1:2015 – *Guide for Electric-Supply Infrastructure to Support Electric Vehicles*, IEEE Standards Association.
5. E. Sortomme, M. A. El-Sharkawi, "Optimal Power Flow Management for Plug-in Hybrid Electric Vehicles," *IEEE Transactions on Smart Grid*, Vol. 2, No. 3, 2011, pp. 416–423.
6. International Energy Agency (IEA) – *Global EV Outlook 2024: Charging Infrastructure and Safety Considerations*, Paris, France.