Otomotiv ile İlgili Güvenlik Açığı veya Saldırı Yöntemleri Listesi

Güvenlik açığı/tehdidin üst düzey ve alt düzey tanımları			*Güvenlik açığı veya saldırı yöntemi örneği*	
4.3.1 Sahadaki araçlarla ilgili arka uç sunuculara yönelik tehditler	1	Bir araca saldırmak veya veri almak için kullanılan arka uç sunucuları	1.1	Personel tarafından ayrıcalıkların kötüye kullanılması (**içeriden saldırı**)
			1.2	**Sunucuya yetkisiz internet erişimi** (örneğin arka kapılar, yamalanmamış sistem yazılımı açıkları, SQL saldırıları veya diğer yollar
			1.3	**Sunucuya yetkisiz fiziksel erişim** (örneğin USB bellekler veya sunucuya bağlanan diğer iletişim araçları tarafından gerçekleştirilen)
	2	Arka uç sunucusundan gelen hizmetlerin kesintiye uğraması, aracın çalışmasını etkilemesi	2.1	**Arka uç sunucuya yapılan saldırı sunucunun çalışmasını durdurulması,** örneğin araçlarla etkileşime girmesini ve ihtiyaç duydukları hizmetleri sağlamasını engeller
	3	Arka uç sunucularda tutulan araçla ilgili verilerin kaybolması veya açığa çıkması ("veri ihlali")	3.1	Personel tarafından ayrıcalıkların kötüye kullanılması (**içeriden saldırı**)
			3.2	**Bulutta bilgi kaybı**. Veriler üçüncü taraf bulut hizmeti sağlayıcıları tarafından depolandığında saldırılar veya kazalar nedeniyle hassas veriler kaybolabilir
			3.3	**Sunucuya yetkisiz internet erişimi** (örneğin arka kapılar, yamalanmamış sistem yazılımı açıkları, SQL saldırıları veya diğer yollarla etkinleştirilir)
			3.4	**Sunucuya yetkisiz fiziksel erişim** (örneğin USB bellekler veya sunucuya bağlanan diğer iletişim araçları tarafından gerçekleştirilen)
			3.5	İstenmeyen veri paylaşımı nedeniyle **bilgi ihlali** (örn. yönetici hataları)
4.3.2 İletişim kanallarına ilişkin araçlara yönelik tehditler	4	Araç tarafından alınan mesajların veya verilerin sahteciliği	4.1	**Kimliğe bürünme yoluyla mesaj sahteciliği** (örneğin, araç takibi sırasında 802.11p (Araçtan herşeye V2X), GNSS (Uydu Konum Belirleme Sistemlerin) deki mesajları, vb.)
			4.2	**Sybil saldırısı** (yolda çok sayıda araç varmış gibi diğer araçları taklit etmek için)
	5	Araçta tutulan kod/veriler üzerinde yetkisiz manipülasyon, silme veya diğer değişiklikleri yapmak için kullanılan iletişim kanalları	5.1	İletişim kanalları **kod enjeksiyonuna** izin verir, örneğin kurcalanmış yazılım ikilisi iletişim akışına enjekte edilebilir
			5.2	İletişim kanalları, araçta tutulan verilerin/kodun **manipüle** edilmesine izin verir

Güvenlik açığı/tehdidin üst düzey ve alt düzey tanımları			*Güvenlik açığı veya saldırı yöntemi örneği*	
			5.3	İletişim kanalları araçta tutulan verilerin/kodun **üzerine yazılmasına** izin verir
			5.4	İletişim kanalları araçta tutulan verilerin/kodun **silinmesine** izin verir
			5.5	İletişim kanalları araca veri/kod girişine izin verir (veri kodu yazma)
	6	İletişim kanallarının güvenilmeyen/güvenilmez mesajların kabul edilmesine izin vermesi veya oturumu ele geçirme/tekrarlama saldırılarına açık olması	6.1	**Güvenilir olmayan veya güvenilmeyen** bir kaynaktan gelen bilgiyi kabul etmek
			6.2	**Ortadaki adam saldırısı/** oturumu ele geçirme
			6.3	**Tekrarlama saldırısı**, örneğin bir iletişim ağ geçidine yönelik bir saldırı, saldırganın bir ECU'nun yazılımının veya ağ geçidinin donanım yazılımının sürümünün düşürmesine olanak tanır
	7	Bilgiler kolayca ifşa edilebilir. Örneğin, iletişimin gizlice dinlenmesi veya hassas dosya veya klasörlere yetkisiz erişime izin verilmesi yoluyla	7.1	**Bilgiye müdahale** / yayınlara müdahale / iletişimin izlenmesi
			7.2	Dosyalara veya verilere **yetkisiz erişim** elde etmek
	8	Araç fonksiyonlarını bozmak için iletişim kanalları üzerinden hizmet reddi saldırıları	8.1	Araç bilgi sistemine **çok sayıda çöp veri gönderilmesi**, böylece **sistemin normal şekilde hizmet verememesi**
			8.2	**Kara delik saldırısı**, araçlar arasındaki iletişimi bozmak için saldırgan araçlar arasındaki mesajları engelleyebilir
	9	Ayrıcalıksız bir kullanıcı araç sistemlerine ayrıcalıklı erişim elde edebilir	9.1	Ayrıcalıksız bir kullanıcı **ayrıcalıklı erişim elde edebilir**, örneğin root erişimi
	10	İletişim ortamına gömülü virüsler araç sistemlerine bulaşabilir	10.1	İletişim ortamına gömülü **virüs** araç sistemlerini etkiler
	11	Araç tarafından alınan (örneğin X2V-(Herseyden araca) veya teşhis mesajları) veya araç içinde iletilen mesajlar kötü amaçlı içerik içerir	11.1	Kötü niyetli **dahili (**örn. CAN**) mesajlar**
			11.2	Kötü niyetli **V2X** mesajları, örneğin altyapıdan araca veya araçtan araca mesajlar (örneğin CAM, DENM)
			11.3	Kötü amaçlı teşhis mesajları
			11.4	Kötü niyetli **özel mesajlar** (örneğin normalde OEM veya bileşen/sistem/işlev tedarikçisinden gönderilenler)
4.3.3. Güncelleme prosedürlerine	12	Güncelleme prosedürlerinin kötüye kullanılması veya tehlikeye atılması	12.1	**Havadan yazılım güncelleme prosedürlerinin t**ehlikeye atılması. Bu, sistem güncelleme programının veya yazılımlarının üretilmesini içerir

Güvenlik açığı/tehdidin üst düzey ve alt düzey tanımları			*Güvenlik açığı veya saldırı yöntemi örneği*	
ilişkin araçlara yönelik tehditler			12.2	**Yerel/fiziksel yazılım güncelleme prosedürlerinin** tehlikeye atılması. Bu, sistem güncelleme programının veya ürün yazılımının üretilmesini içerir
			12.3	**Yazılım güncelleme işleminden önce manipüle** edilmiştir (ve bu nedenle bozulmuştur), ancak güncelleme işlemi bozulmamıştır
			12.4	**Geçersiz güncellemeye izin vermek** için yazılım sağlayıcısının kriptografik anahtarlarının ifşa edilmesi
	13	Meşru güncellemeleri reddetmek mümkündür	13.1	**Kritik yazılım güncellemelerinin yayınlanmasını** ve/veya müşteriye özel özelliklerin kilidinin açılmasını **önlemek için** güncelleme sunucusuna veya ağına karşı Hizmet Reddi saldırısı
4.3.4 Bir siber saldırıyı kolaylaştıran istenmeyen insan eylemlerine ilişkin araçlara yönelik tehditler	15	Meşru aktörler farkında olmadan bir siber saldırıyı kolaylaştıracak eylemlerde bulunabilirler	15.1	Masum kurbanın (örn. mal sahibi, operatör veya bakım mühendisi) istemeden kötü amaçlı yazılım yükleyecek veya bir **saldırıyı etkinleştirecek bir eylemde bulunması için kandırılması**
			15.2	**Tanımlanmış güvenlik prosedürlerine** uyulmaması
4.3.5 Araçların dış bağlantıları ve bağlantıları ile ilgili tehditler	16	Araç fonksiyonlarının bağlantılarının manipüle edilmesi bir siber saldırıya olanak sağlar; buna telematik, uzaktan çalışmaya izin veren sistemler ve kısa menzilli kablosuz iletişim kullanan sistemler dahil olabilir	16.1	Uzaktan anahtar, immobilizer ve şarj istasyonu gibi sistemleri **uzaktan çalıştırmak için tasarlanmış işlevlerin manipülasyonu**
			16.2	**Araç telematiğinin manipülasyonu** (örn. hassas eşyaların sıcaklık ölçümünü manipüle etmek, kargo kapılarının kilidini uzaktan açmak)
			16.3	**Kısa menzilli kablosuz sistemler** veya sensörlerle müdahale
	17	Araç sistemlerine saldırmak için bir araç olarak kullanılan eğlence uygulamaları gibi barındırılan 3. taraf yazılımlar	17.1	Araç sistemlerine saldırmak için bir yöntem olarak kullanılan **bozuk uygulamalar** veya yazılım güvenliği zayıf olanlar
	18	USB portları, OBD portu gibi harici arayüzlere bağlı cihazlar, araç sistemlerine saldırmak için bir araç olarak kullanılır	18.1	USB veya diğer portlar gibi **harici arayüzler**, örneğin kod enjeksiyonu yoluyla bir saldırı noktası olarak kullanılır
			18.2	Bir araç sistemine bağlı **virüs** bulaşmış medya
			18.3	Bir saldırıyı kolaylaştırmak için kullanılan **teşhis erişimi** (örneğin **OBD portundaki dongle'lar**), örneğin araç parametrelerini manipüle etmek (doğrudan veya dolaylı olarak)

Güvenlik açığı/tehdidin üst düzey ve alt düzey tanımları			*Güvenlik açığı veya saldırı yöntemi örneği*	
4.3.6 Araç verilerine/koduna yönelik tehditler	19	Araç verilerinin/kodunun kopyalanması	19.1	Araç sistemlerinden telif hakkı veya tescilli yazılımın kopyalanması (ürün **korsanlığı**)
			19.2	Kişisel veri, ödeme hesabı bilgileri, adres defteri bilgileri, konum bilgileri, aracın elektronik kimliği vb. gibi sahibinin **gizlilik bilgilerine yetkisiz erişim**.
			19.3	Kriptografik anahtarların çıkarılması
	20	Araç verilerinin/kodunun manipülasyonu	20.1	**Aracın elektronik kimliğinde** yasa dışı/yetkisiz değişiklikler
			20.2	**Kimlik sahtekarlığı.** Örneğin, bir kullanıcı ücretli geçiş sistemleriyle iletişim kurarken başka bir kimlik kullanırsa, üretici arka uç
			20.3	**İzleme sistemlerini atlatmaya yönelik eylemler** (örneğin, ODR Takip verileri veya çalışma sayısı gibi mesajların hacklenmesi/ kurcalanması/ engellenmesi)
			20.4	**Aracın sürüş verilerini tahrif etmek** için veri manipülasyonu (örn. kilometre, sürüş hızı, sürüş yönleri, vb.)
			20.5	**Sistem teşhis verilerinde** yetkisiz değişiklikler
	21	Verilerin/kodun silinmesi	21.1	**Sistem olay günlüklerinin** izinsiz silinmesi/manipüle edilmesi
	22	Kötü amaçlı yazılımın tanıtılması	22.2	**Kötü amaçlı yazılım** veya kötü amaçlı yazılım faaliyeti tanıtmak
	23	Yeni yazılımın tanıtılması veya mevcut yazılımın üzerine yazılması	23.1	Araç kontrol sistemi veya bilgi sistemi yazılımının üretimi
	24	Sistemlerin veya operasyonların kesintiye uğraması	24.1	**Hizmet reddi,** örneğin bir CAN veriyoluna mesaj yolu ile baskına neden olarak dahili ağda tetiklenebilir veya yüksek oranda mesajlaşma yoluyla bir ECU'da arızalara neden olabilir
	25	Araç parametrelerinin değiştirilmesi	25.1	Fren verileri, hava yastığı açılma eşiği vb. gibi aracın temel işlevlerinin **yapılandırma parametrelerini tahrif etmek** için yetkisiz erişim.
			25.2	Şarj voltajı, şarj gücü, akü sıcaklığı vb. gibi **şarj parametrelerini tahrif** etmek için yetkisiz erişim.
4.3.7 Yeterince korunmadığı veya sertleştirilmediği takdirde istismar edilebilecek	26	Kriptografik teknolojiler tehlikeye atılabilir veya yeterince uygulanmayabilir	26.1	Kısa şifreleme anahtarları ve uzun geçerlilik süresi kombinasyonu saldırganın **şifrelemeyi** kırmasını sağlar
			26.2	Hassas sistemleri korumak için kriptografik algoritmaların yeterince kullanılmaması

Güvenlik açığı/tehdidin üst düzey ve alt düzey tanımları			*Güvenlik açığı veya saldırı yöntemi örneği*	
potansiyel güvenlik açıkları			26.3	Halihazırda veya yakında kullanımdan kalkacak **kriptografik algoritmaların** kullanılması
	27	Araçların saldırıya uğramasını sağlamak için parçalar veya malzemeler kullanılabilir	27.1	**Bir saldırıyı mümkün kılmak için tasarlanmış** veya bir saldırıyı durdurmak için tasarım kriterlerini karşılamayan **donanım veya yazılım**
	28	Yazılım veya donanım geliştirmeleri güvenlik açıklarına izin verir	28.1	**Yazılım hataları.** Yazılım hatalarının varlığı potansiyel istismar edilebilir güvenlik açıkları için bir temel oluşturabilir. Bu durum özellikle yazılımın bilinen kötü kod/hata bulunmadığını doğrulamak ve bilinmeyen kötü kod/hata bulunması riskini azaltmak için test edilmemiş olması halinde geçerlidir
			28.2	**Geliştirmeden kalanların kullanılması** (örn. hata ayıklama portları, JTAG portları, mikroişlemciler, geliştirme sertifikaları, geliştirici şifreleri, ...) ECU'lara erişime izin verebilir veya saldırganların daha yüksek ayrıcalıklar elde etmesine izin verebilir
	29	Ağ tasarımı güvenlik açıklarını ortaya çıkarır	29.1	Ağ sistemlerine erişim sağlayan **gereksiz internet bağlantı noktalarının açık bırakılması**
			29.2	Kontrol elde etmek için **ağ ayrımını** atlatmak. Korumasız ağ geçitlerinin veya erişim noktalarının (kamyon-treyler ağ geçitleri gibi), koruma sistemlerinin atlatmak ve diğer ağ segmentlerine erişim sağlayarak keyfi CAN veri yolu mesajları göndermek gibi kötü niyetli eylemler gerçekleştirmek için kullanılması özel bir örnektir
	31	İstenmeyen veri aktarımı meydana gelebilir	31.1	Bilgi ihlali. **Araç kullanıcı değiştirdiğinde** (örneğin satıldığında veya yeni kullanıcıları ile kiralık araç olarak kullanıldığında) kişisel veriler sızdırılabilir
	32	Sistemlerin fiziksel olarak manipüle edilmesi bir saldırıyı mümkün kılabilir	32.1	**Elektronik donanımın manipülasyonu**, örneğin "ortadaki adam " saldırısını mümkün kılmak için bir araca eklenen yetkisiz elektronik donanım **Yetkili elektronik donanımın (örn. sensörler) yetkisiz elektronik donanımla** değiştirilmesi **Bir sensör tarafından toplanan bilgilerin manipüle edilmesi** (örneğin, şanzımana bağlı Hall etkisi sensörünü kurcalamak için bir mıknatıs kullanılması)