TRtest
Test ve Değerlendirme A.Ş.

IoT ÜRÜN GRUBU KRİTERLERİ

(Cyber security provisions for consumer IoT)

No	Başlık/Soru	C (Giriş Seviye)	B (Orta Seviye)	A (Üst Seviye)
VPK	**Varsayılan Parola Kullanımı**			
VPK_01	Kullanıcı arayüzlerinde varsayılan parola bulunuyor mu? (Her IoT cihazın kendine özgü parolası olması beklenmektedir.)	C		
VPK_02	Yönetici / Servis arayüzü olan cihazlar için yönetici / cihaz arayüzlerinde varsayılan parola bulunuyor mu? (Yönetici / Servis arayüzlerinde cihazın varsayılan parola yerine kendine özgü parola bulundurması beklenmektedir.)	C		
VPK_03	Güçlü bir parola oluşturma politikası belirlenmiş midir? (En az 10 karakter büyük harf, küçük harf, rakam, özel karakter)	C		
VPK_04	Benzersiz varsayılan parolaların rastgele üretimi sağlanmış mı?		B	
VPK_05	Kullanıcı arayüzleri için varsayılan parolayı değiştirme mekanizması mevcut mu?	C		
VPK_06	Kullanıcı arayüzü için hatalı şifre deneme sayı ve/veya süre kısıtlaması var mı? (Bruteforce vb ataklar gözönüne alınmalıdır.) (En fazla 5 deneme ve / veya 30 dakika blok)		B	
VPK_07	Benzersiz varsayılan parolanın değiştirilmesi zorunlu kılınmış mı?		B	
VPK_08	Cihazın ilk kurulumunda kullanıcı, kullanıcı adı ve parola belirliyor mu?	C		
VPK_09	Kullanım sırasında cihazın konfigurasyonu ile ilgili bir değişiklik yapılması gerektiğinde, kullanıcının cihazda doğrulandıktan sonra cihazın kullanıcıya değişiklik yapmasına izin vermesi sağlanıyor mu?	C		
VPK_10	Cihaz üzerinde kullanıcı doğrulaması sonrasında , kullanıcı ağ servislerinin(UPNP,Dial gibi servisler) devre dışı bırakılması ya da devreye alınması gerçekleştiriliyor mu?	C		
GAR	**Güvenlik Açıklarının Raporlanması**			
GAR_01	Kullanıcılar aldıkları ürün/hizmet üzerinde bulunan güvenlik açıkları hakkında bilgilendiriliyor mu? (Portal, Eposta, SMS - en az biri) (3.taraflardan alınan hizmetler 3.tarafları ilgilendirir.)	C		
GAR_02	Güvenlik açıkları ve ilgili güvenlik yaması hususunda kullanıcı bilgilendiriliyor mu?	C		
GAR_03	Veri sızıntısı durumunda riske giren veriler hakkında bilgilendirme mekanizması mevcut mu?	C		
GAR_04	Güvenlik açıklarının ilgili üreticiye bildirilmesi için üretici tarafından iletişim arayüzü (Coordinated Vulnerability Disclosure CVD) sağlanıyor mu?	C		
GAR_05	Ürün güncelleme stratejisi dokümante edilmiş ve kullanıcıyla paylaşılıyor mu? (güncelleme süreleri, zafiyetin kritiklik derecesine göre güvenlik yama çıkma süreleri, ürüne güncelleme destek süresi- en az bunlar olması gerekir.)	C		
GAR_06	Cihazın fonksiyonel bilgileri üzerinde çalışan ağ servisleri, cihazın topladığı hassas ve kişisel veriler, cihazın bağlandığı bulut bilgileri ve bu buluta aktarılan kişisel ve hassas veriler kullanıcıya şeffaf, anlaşılır bir dokümanla sağlanıyor mu?		B	
GAR_07	Incident Response Plan (Acil Eylem Planı) mevcut mudur?		B	
GAR_08	Cihaz geliştirilirken üretici tarafından "güvenli geliştirme süreçleri" dokümante edilmiş midir? (güvenlikle ilgili optimizasyon ayarları, versiyon kontrol vs)	C		
YGT	**Yazılım Güncellemelerinin Takip Edilmesi**			
YGT_01	Güvenli uzaktan güncelleme fonksiyonları mevcut mudur?		B	
YGT_02	Güvenli manuel güncelleme fonksiyonu mevcut mudur?	C		
YGT_03	Sahadaki cihazların yazılım güncellemeleri takip ediliyor mu ?		B	
YGT_04	Yazılım versiyon düşürmeye karşı güvenlik var mı?	C		
YGT_05	Yazılım güncelleme paketleri güvenli bir kanal üzerinden cihaza aktarılıyor mu?	C		
YGT_06	Yazılım güncelleme dosyaları NIST tarafından onaylı algoritmalar kullanılarak imzalanıyor mu ?		B	
YGT_07	Yazılım güncelleme paketleri tersine mühendislik saldırılarına karşı güvenli mi ?		B	
YGT_08	Herhangi bir çalışma anında cihazın yazılım güncellemesi kontrolü yapılıyor mu?		B	

YGT_09	Bir güncelleme yayınlandığında cihazların hepsine aynı anda değil de belirli aralıklar koyularak, gruplanarak gönderiliyor mu?		B	
YGT_10	IoT cihazları veya IoT cihazlarının internete bağlanmasında kullanılan gateway (mobil uygulama, z-wave, zigbee vs) güncelleme sorgusunu rastgele aralıklarla yapıyor mu?		B	
KGPS	**Kritik Güvenlik Parametrelerinin Güvenli Bir Şekilde Saklanması**			
KGPS_01	Kritik güvenlik parametrelerinin güvenliği için özel bir donanım altyapısı kullanılıyor mu? (HSM, TEE, Trust zone, vb)		B	
KGPS_02	Cihaza özel sertifika, eşsiz anahtarların cihaza yüklendiği aşamada güvenli bir üretim altyapısı ve süreci devreye alındığı dokümante edilmiş midir?			A
KGPS_03	Her bir cihaz için eşsiz bir kimliklendirme mevcut mudur?		B	
KGPS_04	Donanım yerine ürün yazılımına gömülmüş güvenlik parametrelerinin kullanımı engellenmiş mi?		B	
KGPS_05	Yazılım güncelleme esnasındaki integrity ve authentication adımlarının kullandığı güvenlik parametreleri her cihaz için eşsiz mi?		B	
HG	**Haberleşme Güvenliği**			
HG_01	Cihazda NIST Onaylı TLS ve Güvenli Cipher Suite ler kullanılıyor ve destekleniyor mu? (TLS 1.2 , TLS 1.3)	C		
HG_02	Haberleşme güvenliği ile ilgili yazılımsal kriptografik modüller ve algoritmalar güncellenebiliyor mu ? (SSL Kütüphaneleri) (cryptoagility)		B	
HG_03	Kriptografik algoritmaların güncellenemediği ürünlerde, algoritmaların ömrü ve geçerliliği ürün ömründen uzun mu?			A
HG_04	Cihaz bulut haberleşmesinde çift yönlü kimlik doğrulama (client ve sunucu sertifikaları doğrulaması) ile haberleşme güvenliği sağlanıyor mu? (Mutual authentication)		B	
HG_05	Cihaza aktarılmak durumunda kalan güvenlik parametreleri uygun, güncel ve uluslararası geçerliliği olan encryption algoritmalarıyla şifreleniyor mu? (confidentiality)		B	
HG_06	Yaşam döngüsü (Üretim süreçleri dahil) boyunca gözden geçirilmiş, uluslararası "anahtar yönetimi"süreçleri kullanılıyor mu?			A
HG_07	Anahtar üretiminde güvenli donanım altyapıları kullanılıyor mu?(HSM Back-end) (BU MADDE İLERİ SEVİYE DÜŞÜNÜLÜYOR)			A
AYME	**Atak Yüzeylerinin Minimize Edilmesi**			
AYME_01	Kullanılmayan tüm network ve arayüzler (Örneğin TCP,UDP Portlar/local network servisleri) kapatılmı	C		
AYME_02	Cihazın ilk kurulumunda cihaza ait bilgiler kullanıcı kimlik doğrulaması olmadan paylaşılıyor mu?		B	
AYME_03	Cihaz ilk açıldığı anda kullanıcının izni olmadan güvenlik ve gizlilik ihlaline neden olabilecek bilgiler paylaşılıyor mu?	C		
AYME_04	Test ve debug amaçlı hiçbir yazılım/donanım arayüzünün açık bırakılmadığı garanti edilmiş mi?	C		
AYME_05	Cihazda bir debug arayüzüne erişilebiliniyorsa, bunun yazılımsal olarak kapalı olduğu garanti altına alınmış mı ?	C		
AYME_06	Cihaz yazılımında bulunan bileşenler üzerinde bilinen kritik zafiyetler mevcut mudur?	C		
AYME_07	Cihaz üzerindeki servisler ve prosesler minumum sistem yetkileri ile mi çalışıyor? (Root kullanıcısı altında çalışmamalıdır.)	C		
AYME_08	Cihaz üzerinde yatay ve dikey yetki artırımı saldırılarına karşı önlem alınmış mıdır?		B	
YBS	**Yazılım Bütünlüğünü Sağlama**			
YBS_01	Tüketici IoT cihazı, güvenli önyükleme mekanizmaları kullanarak yazılımını doğruluyor mu?		B	
YBS_02	Yazılımda yetkisiz bir değişiklik tespit edilirse, cihaz kullanıcıyı ve / veya yöneticiyi sorun konusunda uyarıyor mu?			A
YBS_03	Uyarıların sadece kullanıcıya ve/veya üreticiye yönlendirildiğinden emin olunuyor mu?			A
YBS_04	Cihaz üzerindeki servislerin ve proseslerin bütünlüğü kontrol edilerek çalıştırılıyor mu?		B	
YBS_05	Cihaz üzerinde çalışan cihaz yazılımı, servis ve proseslerin bütünlüğü ile ilgili problem olduğunda özel güvenlik moduna geçiş sağlıyor mu?			A
KBS	**Kişisel Veri Bütünlüğünü Sağlama**			
KBS_01	Cihaz içerisinde saklanan ve cihaz dışına aktarılan kişisel verilerin gizliliği güncel ve uluslararası geçerliliği olan yöntemler ile korunuyor mu?		B	
KBS_02	Cihazın kişisel veri ile ilgili harici algılama yetenekleri (kamera, mikrofon), kullanıcı için açık ve şeffaf, erişilebilir bir şekilde dokümante edilmiş midir?		B	
SKDH	**Sistemleri Kesintilere Karşı Dayanıklı Hale Getirme**			
SKDH_01	Cihaz tam özellikli çalışabilmek için bir ağ bağlantısına ihtiyaç duyuyor mu? Ağ bağlantısı kesildiği takdirde cihazın güvenlik ile ilgili özellikleri eksiksiz çalışıyor mu?	C		

SKDH_02	Enerji kesintisi sonrası sistem durumunu kaydedip varolan güvenlik prosedürlerine devam edebiliyor r	C		
SKDH_03	IoT cihazlarına yönelik yapılan DOS atakları sonrasında data expose(veri ifşası) ortaya çıkıyor mu?			A
SKDH_04	DOS atak sonrasında IoT cihaz güvenlik mekanizmalarından ödün vermeden recovery mekanizmasını barındırıyor mu?			A
SKDH_05	IoT cihazı herhangi bir servis kesintisi durumunda alarm üretiyor mu ?		B	
STVT	**Sistem Telemetri Verilerini İnceleme**			
STVT_01	Cihazlardan telemetri verileri toplanması durumunda, bu veriler güvenlik anomalilerini tespit amacıyla kullanılabiliyor mu?			A
STVT_02	Telemetri verilerinden anomali tespiti oluştuğunda kullanıcıya/üreticiye alarm üretiliyor mu?(bilgilendirme)			A
KKVSK	**Kullanıcıların Kullanıcı Verilerini Silmesini Kolaylaştırma**			
KKVSK_01	Kullanıcılar istediklerinde kendi verilerini cihazdan kaldırabiliyor mu ? (kişisel veri, kullanıcı konfigürasyonu ve parola benzeri kriptografik materyaller)	C		
KKVSK_02	Kullanıcılara verilerinin kaldırıldığından emin olabileceklerini sağlayan bir bildirim veriliyor mu?		B	
KKVSK_03	Kullanıcılar kiralık ya da geçici kullanım cihazlarda kullanıcı verilerini cihazı sıfırlamadan silebiliyor mu?		B	
KKVSK_04	Kullanıcılar, kendi verilerini nasıl kaldıracakları konusunda yönlendiriliyor mu?		B	
CKBK	**Cihaz Kurulumu ve Bakımını Kolaylaştırma**			
CKBK_01	Ürün, kurulum esnasında kullanıcılara doğru konfigürasyon ve güvenlik ayarlarını yapılandırmada yardımcı oluyor mu?		B	
CKBK_02	Üretici, kullanıcılara güvenli kurulum amacı ile kurulum talimatlarını bildiriyor mu?		B	
CKBK_03	Üretici, kullanıcılara kurulumdan sonra güvenli kurulum talimatlarının izlendiğinden emin olabileceği bir yöntem sağlıyor mu?		B	
GVD	**Giriş Verilerini Doğrulama**			
GVD_01	Input noktası sadece işlemesi gerektiği(alfanümerik, özel karakter vb) formattaki veri tipini mi kabul ediyor?	C		
GVD_02	Input validation yaklaşımında white-listing kullanılıyor mu?		B	
GVD_03	Injection, Buffer Overflow gibi kötücül kaynaklardan gelen ataklara karşı input validation yaklaşımı kullanılıyor		B	