ETSI EN 303 645-TS 103 701

1. Cihaz ve sistemlerde varsayılan parola kullanılmamalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.1, ETSI TS 103 701 - Madde 5.1)

Tüm cihazlar benzersiz, güçlü ve varsayılan olmayan parolalarla gelmelidir.

(ETSI EN 303 645 - Madde 5.1.1, ETSI TS 103 701 - Madde 5.1.1.1)

Kullanıcıların güvenli şifreler oluşturması teşvik edilmelidir.

(ETSI EN 303 645 - Madde 5.1.2, ETSI TS 103 701 - Madde 5.1.1.2)

Kimlik doğrulama mekanizmaları MFA (Çok Faktörlü Kimlik Doğrulama) desteklemelidir.

(ETSI TS 103 701 - Madde 5.1.5)

2. Güvenlik Açığı Bildirim Mekanizması Oluşturulmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.2, ETSI TS 103 701 - Madde 5.2)

Siber güvenlik açıklarının raporlanmasını sağlayan bir kanal (örn. Siber güvenlik işlemleri veya güvenlik ekibi için e-posta) oluşturulmalıdır.

(ETSI EN 303 645 - Madde 5.2.1, ETSI TS 103 701 - Madde 5.2.1.1)

Açıkların belirlenmesi ve düzeltilmesi için düzenli güvenlik testleri yapılmalıdır.

(ETSI TS 103 701 - Madde 5.2.2)

3. Yazılımlar güncel tutulmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.3, ETSI TS 103 701 - Madde 5.3)

Cihazların yazılım güncellemeleri düzenli olarak sağlanmalı ve eski sürümler için destek belirli bir süre devam etmelidir.

(ETSI EN 303 645 - Madde 5.3.1, ETSI TS 103 701 - Madde 5.3.1.1)

Güncellemeler otomatik olarak veya kullanıcı dostu bir şekilde sunulmalıdır.

(ETSI EN 303 645 - Madde 5.3.2, ETSI TS 103 701 - Madde 5.3.3)

Güncellemeler güvenilir kaynaklardan indirilmeli ve kurulum sırasında doğrulanmalıdır.

(ETSI EN 303 645 - Madde 5.3.4, ETSI TS 103 701 - Madde 5.3.6)

4. Hassas güvenlik parametreleri güvenli şekilde saklanmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.4, ETSI TS 103 701 - Madde 5.4)

Şifreler ve kimlik doğrulama bilgileri gibi hassas veriler şifrelenmiş olarak saklanmalıdır.

(ETSI EN 303 645 - Madde 5.4.1, ETSI TS 103 701 - Madde 5.4.1.1)

Güvenlik sertifikaları düzenli olarak güncellenmeli ve saklama alanları koruma altına alınmalıdır.

(ETSI TS 103 701 - Madde 5.4.3)

5. İletişim güvenli şekilde yapılmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.5, ETSI TS 103 701 - Madde 5.5)

Tüm ağ bağlantıları TLS (Transport Layer Security) veya benzeri güvenlik protokolleri kullanılarak şifrelenmelidir.

(ETSI EN 303 645 - Madde 5.5.1, ETSI TS 103 701 - Madde 5.5.1.1)

Hassas verilerin açık metin halinde iletilmemesi sağlanmalıdır.

(ETSI EN 303 645 - Madde 5.5.2, ETSI TS 103 701 - Madde 5.5.2.1)

Cihazlar, yalnızca güvenilir sertifikalara sahip sistemlerle iletişim kurmalıdır.

(ETSI TS 103 701 - Madde 5.5.3)

6. Siber güvenlik atak yüzeyi minimize edilmelidir.

(Kaynak: ETSI EN 303 645 - Madde 5.6, ETSI TS 103 701 - Madde 5.6)

Kullanılmayan servisler devre dışı bırakılmalı ve gereksiz portlar kapatılmalıdır.

(ETSI EN 303 645 - Madde 5.6.1, ETSI TS 103 701 - Madde 5.6.1.1)

Varsayılan olarak cihazlar, minimum izinlerle çalışacak şekilde yapılandırılmalıdır.

(ETSI EN 303 645 - Madde 5.6.2, ETSI TS 103 701 - Madde 5.6.2.1)

Saldırı vektörlerini azaltmak için erişim kontrolleri uygulanmalıdır.

(ETSI TS 103 701 - Madde 5.6.5)

7. Yazılımların bütünlüğü güvence altına alınmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.7, ETSI TS 103 701 - Madde 5.7)

Firmware ve yazılım bütünlüğünü doğrulamak için dijital imzalama teknikleri kullanılmalıdır.

(ETSI EN 303 645 - Madde 5.7.1, ETSI TS 103 701 - Madde 5.7.1.1)

Yazılım değişiklikleri yalnızca yetkilendirilmiş kullanıcılar tarafından yapılabilmelidir.

(ETSI EN 303 645 - Madde 5.7.2, ETSI TS 103 701 - Madde 5.7.2.1)

Yetkisiz erişimi engellemek için cihaz üzerinde güvenlik mekanizmaları uygulanmalıdır.

(ETSI TS 103 701 - Madde 5.7.3)

8. Kişisel verinin güvenliği sağlanmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.8, ETSI TS 103 701 - Madde 5.8)

GDPR ve benzeri veri koruma yönetmeliklerine uyum sağlanmalıdır.

(ETSI EN 303 645 - Madde 5.8.1, ETSI TS 103 701 - Madde 5.8.1.1)

Kullanıcı verileri minimum seviyede toplanmalı ve yalnızca gerekli durumlarda kullanılmalıdır.

(ETSI EN 303 645 - Madde 5.8.2, ETSI TS 103 701 - Madde 5.8.2.1)

Cihazlar, kullanıcıların kişisel verilerini kolayca silebilmesine olanak tanımalıdır.

(ETSI TS 103 701 - Madde 5.8.3)

9. Sistemler kesintilere dayanıklı hale getirilmelidir.

(Kaynak: ETSI EN 303 645 - Madde 5.9, ETSI TS 103 701 - Madde 5.9)

Cihazlar, ani elektrik kesintilerine ve bağlantı kayıplarına karşı dayanıklı olmalıdır.

(ETSI EN 303 645 - Madde 5.9.1, ETSI TS 103 701 - Madde 5.9.1.1)

Kritik işlevler için yedekleme sistemleri veya failover mekanizmaları uygulanmalıdır.

(ETSI TS 103 701 - Madde 5.9.2)

10. Sistem telemetri verileri incelenmelidir.

(Kaynak: ETSI EN 303 645 - Madde 5.10, ETSI TS 103 701 - Madde 5.10)

Cihazın performansını ve güvenlik durumunu izleyen telemetri mekanizmaları sağlanmalıdır.

(ETSI EN 303 645 - Madde 5.10.1, ETSI TS 103 701 - Madde 5.10.1.1)

Kullanıcı gizliliğine uygun şekilde loglama yapılmalı ve şüpheli aktiviteler tespit edilmelidir.

(ETSI TS 103 701 - Madde 5.10.2)

11. Kullanıcıların kendi verilerini kolayca silebilmesi sağlanmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.11, ETSI TS 103 701 - Madde 5.11)

Kullanıcılar, kişisel verilerini cihazdan tamamen silebilmelidir.

(ETSI EN 303 645 - Madde 5.11.1, ETSI TS 103 701 - Madde 5.11.1.1)

Silme işlemi, geri döndürülemez şekilde ve güvenli bir şekilde gerçekleştirilmelidir.

(ETSI TS 103 701 - Madde 5.11.2)

12. Cihazların kurulumu ve bakımı kolaylaştırılmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.12, ETSI TS 103 701 - Madde 5.12)

Kullanıcıların güvenli şifreler ve güncellemeleri kolayca yapabilmesini sağlayan arayüzler sunulmalıdır.

(ETSI EN 303 645 - Madde 5.12.1, ETSI TS 103 701 - Madde 5.12.1.1)

Cihazların fabrika ayarlarına güvenli bir şekilde sıfırlanabilmesi sağlanmalıdır.

(ETSI TS 103 701 - Madde 5.12.3)

13. Girdi verileri doğrulanmalıdır.

(Kaynak: ETSI EN 303 645 - Madde 5.13, ETSI TS 103 701 - Madde 5.13)

Kullanıcı girdileri, enjeksiyon saldırılarına (SQL Injection, XSS vb.) karşı korunmalıdır.

(ETSI EN 303 645 - Madde 5.13.1, ETSI TS 103 701 - Madde 5.13.1.1)

Veri doğrulama mekanizmaları geliştirilerek yalnızca beklenen türdeki verilerin işlenmesi sağlanmalıdır.

(ETSI TS 103 701 - Madde 5.13.2)

1.1 Donanım Güvenlik Analizleri

Bir IoT ürünündeki gömülü cihaz, kullanıcı senaryosuna bağlı olarak birkaç farklı amaç için kullanılabilir. Cihazın tüm IoT mimarisi için bir merkez olarak kullanılabilir, fiziksel çevresinden veri toplayan sensör olarak hizmet edebilir veya verileri görüntülemenin veya kullanıcı tarafından amaçlanan eylemi gerçekleştirmenin bir yolu olarak kullanılabilir. Testler donanımın kullanım görevine göre şekillendirilecek olmakla beraber, aşağıdaki temel başlıklar kapsamında değerlendirilecektir.

- Seri bağlantı noktalarından yetkisiz erişim saldırıları
- Seri portlarda kullanılan güvensiz kimlik doğrulama mekanizmaları testleri
- Firmware'i JTAG veya Flash çipleri üzerinden boşaltma yeteneği
- Dış medya tabanlı saldırılar

1.2 Uygulama Güvenlik Analizleri

Cihaz/Sistemin bağlı olduğu Mobil/Masaüstü/Web Uygulamalarında kullanılacak farklı kullanıcı tipleri göz önüne alınarak gerçekleştirecektir. Bu kapsamda, yapılacak denetlemeler aşağıda detaylı olarak açıklanmıştır.

- Uygulamada tersine mühendislik çalışmaları
- Uygulamanın kaynak kod incelemesi (Kapsama dahil ise uygulanır.)
- Güvensiz kimlik doğrulama ve yetkilendirme kontrolleri
- Input Doğrulama Değerlendirmeleri
- İş ve mantık kusurları
- Zaman manipülasyon saldırıları
- Güvensiz ağ iletişimi saldırıları
- Güvensiz Sürüm üçüncü taraf kitaplıkları ve yazılım geliştirme kitleri (SDK'lar)

1.3 Firmware Analizleri

İncelenen bileşen, cihazda çalışan bellenimden, cihazı kontrol etmek için kullanılan mobil uygulamalardan, cihaza bağlı bulut bileşenlerine kadar her şeyi içeren yazılımdır. Geleneksel sızma testi deneyiminin IoT ekosistemine uygulandığı bazı bölümleri de içerir. Gelişmiş RISC Makineleri (ARM) ve MIPS (Kilitli Boru Hatlı Aşamaları olmayan Mikroişlemci) dahil olmak üzere farklı mimarideki ikili dosyaların tersine mühendisliğinin yanı sıra cihaz üzerinde çalışan mobil uygulamaların tersine mühendisliği gibi konuları içerecektir.

Firmware incelemelerinde bakılacak bazı açıklıklar aşağıda listelenmiştir.

- Bellenimi değiştirme yeteneği.
- Güvensiz imza ve bütünlük doğrulaması.
- Donanım yazılımında sabit kodlanmış hassas değerler — (API anahtarları, parolalar, URL'ler vb.)
- Özel sertifikalar.
- Firmware aracılığıyla cihazın tüm işlevselliğini anlama yeteneği.

1.4 Radyo İletişim Protokol Analizleri

Hücresel, WI-Fi, BLE, ZigBee, Wave, 6LoWPAN, LoRa ve daha fazlasının kullanıldığı çeşitli radyo iletişim protokolleri vardır. Test Cihazının hangi iletişim protokolünü kullandığına bağlı olarak Radyo iletişiminin analizini gerçekleştirmek için özel donanımlarla yapılan analiz senaryolarını içerir.

- Ortadaki adam saldırıları.
- Tekrar tabanlı saldırılar.
- Güvensiz Döngüsel Artıklık Kontrolü (CRC) doğrulaması.
- Sıkışma tabanlı saldırılar (Roll-jam saldırısı).
- Hizmet reddi (DoS).
- Şifreleme eksikliği (ADB-S Paketi).
- Radyo paketlerinden hassas bilgileri çıkarma yeteneği (GQRX veya GNU Radyo).
- Canlı radyo iletişiminin durdurulması ve değiştirilmesi.