

Nechh Eco-Report

Hazırlık belgesi — resmî kullanımdan önce gözden geçirilmelidir · Preparation document — review required before official use

ÖRNEK RAPOR — GEÇERSİZDİR. Bu rapor kurgusal bir firma ve kurgusal verilerle, gerçek raporla aynı hesap motoru ve aynı biçimle üretilmiştir. Hiçbir resmî işlemde, beyanda veya alıcıya sunumda kullanılamaz. Sizin raporunuz kendi verilerinizle üretilir, firmanızın adıyla filigranlanır ve Rapor No'su doğrulama adresinden kontrol edilebilir.

CRA Ürün ve Uygunluk Raporu

Bu bir HAZIRLIK değerlendirmesidir: CE işareti, AB uygunluk beyanı ya da onaylanmış kuruluş incelemesi yerine geçmez. Ürün sınıfı ve uygunluk yolu nihai olarak ürünün teknik özelliklerine göre belirlenir.

Rapor No: ÖRNEK-GEÇERSİZ

Hazırlanma (UTC): 2026-10-26T00:17:13Z

Firma: ÖRNEK FİRMA A.Ş. (kurgusal)

1. Sonuç

- **Karar:** Ek III Sınıf II — üçüncü taraf değerlendirmesi şart
- **Gerekçe:** Ek III Sınıf II önemli ürün (2. Firewalls, intrusion detection and prevention systems): md. 32(3) uyarınca üçüncü taraf (onaylanmış kuruluş) değerlendirmesi gerekir; iç kontrol yetmez.
- **Dayanak maddeler:** Article 32(3)
- **Değerlendirme tarihi:** 2026-10-26

2. Eksik cevaplar

Aşağıdaki sorular cevaplanmadı. Cevaplanmayan soru "hayır" sayılmaz; tamamlanınca rapor yeniden alınmalıdır.

- Md. 14(2)(a) — Erken uyarı 24 saat içinde gönderilebiliyor
- Md. 14(2)(b) — Zafiyet/olay bildirimi 72 saat içinde gönderilebiliyor
- Md. 14(2)(c) — Nihai rapor süresi içinde gönderilebiliyor
- Articles 29-30 — CE işareti kurallara uygun şekilde iliştilmiş
- Annex I Part II (5) — Koordineli zafiyet açıklama politikası yayımlanmış
- Md. 28 + Annex V — AB uygunluk beyanı düzenlenmiş
- (a) — Bilinen, istismar edilebilir zafiyet olmadan piyasaya sunulmalı
- (b) — Varsayılan olarak güvenli yapılandırma ile sunulmalı; ürünü ilk hâline döndürme imkânı olmalı (özel ürünlerde üretici-işletme anlaşması saklı)
- (c) — Zafiyetler güvenlik güncellemeleriyle giderilebilmeli; uygun hâllerde varsayılan açık otomatik güncelleme, kolay kapatma, güncelleme bildirimi ve erteleme imkânı
- (d) — Uygun kontrol mekanizmalarıyla (kimlik doğrulama, kimlik/erişim yönetimi) yetkisiz erişime karşı korunmalı ve olası yetkisiz erişimi bildirmeli
- (e) — Saklanan, iletilen veya işlenen verinin gizliliği korunmalı (ör. güncel tekniklerle şifreleme)
- (f) — Veri, komut, program ve yapılandırmanın bütünlüğü yetkisiz değişikliğe karşı korunmalı; bozulmalar bildirilmeli

- (g) — Yalnızca amaca yeterli, ilgili ve gerekli veri işlenmeli (veri minimizasyonu)
- (h) — Temel işlevlerin erişilebilirliği olay sonrasında da korunmalı (hizmet engelleme saldırılarına karşı dayanıklılık dahil)
- (i) — Ürünün veya bağlı cihazların başka cihaz ve ağların hizmetlerine olumsuz etkisi en aza indirilmeli
- (j) — Saldırı yüzeyini (dış arayüzler dahil) sınırlayacak şekilde tasarlanmalı, geliştirilmeli ve üretilmeli
- (k) — Uygun istismar önleme mekanizmalarıyla bir olayın etkisini azaltacak şekilde tasarlanmalı
- (l) — İlgili iç etkinlikleri (veri, hizmet ve işlevlere erişim ve değişiklik) kaydederek güvenlik bilgisi sağlamalı; kullanıcı bunu kapatabilmeli
- (m) — Kullanıcı tüm veri ve ayarları kalıcı ve güvenli biçimde silebilmeli; veri başka ürüne aktarılabilirse bu güvenli yapılmalı
- (1) — Üründeki zafiyetleri ve bileşenleri belirleyip belgelemek; en az üst düzey bağımlılıkları kapsayan, makinece okunabilir yazılım malzeme listesi (SBOM) hazırlamak
- (2) — Zafiyetleri gecikmeden gidermek (güvenlik güncellemesiyle); mümkünse güvenlik güncellemelerini işlev güncellemelerinden ayrı sunmak
- (3) — Ürün güvenliğini etkili ve düzenli olarak test etmek ve gözden geçirmek
- (4) — Güncelleme yayımlandıktan sonra giderilen zafiyetleri (açıklama, etkilenen ürün, etki, ciddiyet, giderme yolu) kamuya açıklamak; haklı hâllerde kullanıcılar yamayı uygulayana kadar ertelemek
- (5) — Koordineli zafiyet bildirimi politikası oluşturmak ve uygulamak
- (6) — Ürün ve içindeki üçüncü taraf bileşenlerin zafiyetlerine ilişkin bilgi paylaşımını kolaylaştırmak; zafiyet bildirimi için iletişim adresi sağlamak
- (7) — Güncellemelerin güvenli dağıtımı için mekanizma kurmak; güvenlik güncellemelerinde uygun hâllerde otomatik dağıtım
- (8) — Güvenlik güncellemelerini gecikmeden ve (özel ürün anlaşması hariç) ücretsiz dağıtmak; kullanıcıya yapılacak işlemi anlatan bilgilendirme eklemek
- Md. 13(2)-(4) — Siber güvenlik risk değerlendirmesi yapılmış ve teknik dosyaya konmuş
- Annex I Part II (1) — Yazılım bileşen listesi (SBOM) tutuluyor
- Annex I Part II (8) — Güvenlik güncellemeleri ücretsiz ve gecikmesiz dağıtılıyor
- Md. 13(8) — Destek süresi belirlenmiş ve satın alma anında açıkça yazılı
- Md. 31 + Annex VII — Teknik dosya Ek VII'deki içerikle hazır
- Md. 14(8) — Kullanıcıları bilgilendirme süreci var

3. Yükümlülükler ve kontrol listeleri

Ek I Kısım I — ürün gereklilikleri

Hazır 0 / 13 · eksik 0 · cevaplanmadı 13

- **(a)** Bilinen, istismar edilebilir zafiyet olmadan piyasaya sunulmalı — Cevaplanmadı
- Resmî metin: be made available on the market without known exploitable vulnerabilities
- **(b)** Varsayılan olarak güvenli yapılandırma ile sunulmalı; ürünü ilk hâline döndürme imkânı olmalı (özel ürünlerde üretici-işletme anlaşması saklı) — Cevaplanmadı
- Resmî metin: be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state
- **(c)** Zafiyetler güvenlik güncellemeleriyle giderilebilmeli; uygun hâllerde varsayılan açık otomatik güncelleme, kolay kapatma, güncelleme bildirimi ve erteleme imkânı — Cevaplanmadı

- Resmî metin: ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of availability
- **(d)** Uygun kontrol mekanizmalarıyla (kimlik doğrulama, kimlik/erişim yönetimi) yetkisiz erişime karşı korunmalı ve olası yetkisiz erişimi bildirmeli — Cevaplanmadı
- Resmî metin: ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access
- **(e)** Saklanan, iletilen veya işlenen verinin gizliliği korunmalı (ör. güncel tekniklerle şifreleme) — Cevaplanmadı
- Resmî metin: protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means
- **(f)** Veri, komut, program ve yapılandırmanın bütünlüğü yetkisiz değişikliğe karşı korunmalı; bozulmalar bildirilmeli — Cevaplanmadı
- Resmî metin: protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions
- **(g)** Yalnızca amaca yeterli, ilgili ve gerekli veri işlenmeli (veri minimizasyonu) — Cevaplanmadı
- Resmî metin: process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)
- **(h)** Temel işlevlerin erişilebilirliği olay sonrasında da korunmalı (hizmet engelleme saldırılarına karşı dayanıklılık dahil) — Cevaplanmadı
- Resmî metin: protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks
- **(i)** Ürünün veya bağlı cihazların başka cihaz ve ağların hizmetlerine olumsuz etkisi en aza indirilmeli — Cevaplanmadı
- Resmî metin: minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks
- **(j)** Saldırı yüzeyini (dış arayüzler dahil) sınırlayacak şekilde tasarlanmalı, geliştirilmeli ve üretilmeli — Cevaplanmadı
- Resmî metin: be designed, developed and produced to limit attack surfaces, including external interfaces
- **(k)** Uygun istismar önleme mekanizmalarıyla bir olayın etkisini azaltacak şekilde tasarlanmalı — Cevaplanmadı
- Resmî metin: be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques
- **(l)** İlgili iç etkinlikleri (veri, hizmet ve işlevlere erişim ve değişiklik) kaydederek güvenlik bilgisi sağlamalı; kullanıcı bunu kapatabilmeli — Cevaplanmadı
- Resmî metin: provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user
- **(m)** Kullanıcı tüm veri ve ayarları kalıcı ve güvenli biçimde silebilmeli; veri başka ürüne aktarılabilirse bu güvenli yapılmalı — Cevaplanmadı
- Resmî metin: provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Ek I Kısım II — zafiyet yönetimi

Hazır 0 / 8 · eksik 0 · cevaplanmadı 8

- **(1)** Üründeki zafiyetleri ve bileşenleri belirleyip belgelemek; en az üst düzey bağımlılıkları kapsayan, makinece okunabilir yazılım malzeme listesi (SBOM) hazırlamak — Cevaplanmadı
- Resmî metin: identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products
- **(2)** Zafiyetleri gecikmeden gidermek (güvenlik güncellemesiyle); mümkünse güvenlik güncellemelerini işlev güncellemelerinden ayrı sunmak — Cevaplanmadı
- Resmî metin: in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates
- **(3)** Ürün güvenliğini etkili ve düzenli olarak test etmek ve gözden geçirmek — Cevaplanmadı
- Resmî metin: apply effective and regular tests and reviews of the security of the product with digital elements
- **(4)** Güncelleme yayımlandıktan sonra giderilen zafiyetleri (açıklama, etkilenen ürün, etki, ciddiyet, giderme yolu) kamuya açıklamak; haklı hâllerde kullanıcılar yamayı uygulayana kadar ertelemek — Cevaplanmadı
- Resmî metin: once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity a
- **(5)** Koordineli zafiyet bildirim politikası oluşturmak ve uygulamak — Cevaplanmadı
- Resmî metin: put in place and enforce a policy on coordinated vulnerability disclosure
- **(6)** Ürün ve içindeki üçüncü taraf bileşenlerin zafiyetlerine ilişkin bilgi paylaşımını kolaylaştırmak; zafiyet bildirim için iletişim adresi sağlamak — Cevaplanmadı
- Resmî metin: take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product wi
- **(7)** Güncellemelerin güvenli dağıtımı için mekanizma kurmak; güvenlik güncellemelerinde uygun hâllerde otomatik dağıtım — Cevaplanmadı
- Resmî metin: provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner
- **(8)** Güvenlik güncellemelerini gecikmeden ve (özel ürün anlaşması hariç) ücretsiz dağıtmak; kullanıcıya yapılacak işlemi anlatan bilgilendirme eklemek — Cevaplanmadı
- Resmî metin: ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory mes

Üretici yükümlülükleri

Hazır 0 / 8 · eksik 0 · cevaplanmadı 8

- **Md. 13(2)-(4)** Siber güvenlik risk değerlendirmesi yapılmış ve teknik dosyaya konmuş — Cevaplanmadı
- **Md. 31 + Annex VII** Teknik dosya Ek VII'deki içerikle hazır — Cevaplanmadı
- **Md. 28 + Annex V** AB uygunluk beyanı düzenlenmiş — Cevaplanmadı
- **Articles 29-30** CE işareti kurallara uygun şekilde iliştilirilmiş — Cevaplanmadı
- **Annex I Part II (1)** Yazılım bileşen listesi (SBOM) tutuluyor — Cevaplanmadı
- **Annex I Part II (5)** Koordineli zafiyet açıklama politikası yayımlanmış — Cevaplanmadı
- **Annex I Part II (8)** Güvenlik güncellemeleri ücretsiz ve gecikmesiz dağıtılıyor — Cevaplanmadı
- **Md. 13(8)** Destek süresi belirlenmiş ve satın alma anında açıkça yazılı — Cevaplanmadı

Bildirim hazırlığı

- **Md. 14(2)(a)** Erken uyarı 24 saat içinde gönderilebiliyor — Cevaplanmadı
- **Md. 14(2)(b)** Zafiyet/olay bildirimi 72 saat içinde gönderilebiliyor — Cevaplanmadı
- **Md. 14(2)(c)** Nihai rapor süresi içinde gönderilebiliyor — Cevaplanmadı
- **Md. 14(8)** Kullanıcıları bilgilendirme süreci var — Cevaplanmadı

Ek VII teknik dosya kalemleri

- **1** Ürünün genel tanımı
- Resmî metin: a general description of the product with digital elements, including:
- **2** Ürünün tasarım, geliştirme ve üretimi ile zafiyet yönetim süreçlerinin tanımı
- Resmî metin: a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:
- **3** Siber güvenlik risk değerlendirmesi (md. 13) ve Ek I Bölüm I gerekliliklerinin nasıl uygulandığı
- Resmî metin: an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;
- **4** Destek süresinin belirlenmesinde dikkate alınan bilgiler (md. 13(8))
- Resmî metin: relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;
- **5** Tamamen veya kısmen uygulanan uyumlaştırılmış standartların listesi
- Resmî metin: a list of the harmonised standards applied in full or in part the references of which have been published in the
- **6** Ek I Bölüm I ve II gerekliliklerine uygunluğu doğrulayan test raporları
- Resmî metin: reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;
- **7** AB uygunluk beyanının kopyası
- Resmî metin: a copy of the EU declaration of conformity;
- **8** Uygun hâllerde, piyasa gözetim otoritesinin gerekçeli talebi üzerine yazılım malzeme listesi (SBOM)
- Resmî metin: where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.

4. Diğer bilgiler

- **AB pazarına sunuluyor:** evet
- **Ürün sınıfı:** Ek III Sınıf II

Ürün kategorisi

- **No:** 2
- **Başlık:** Firewalls, intrusion detection and prevention systems
- **EHR sistemi:** hayır
- **Kapsam dışı gerekçesi:** belirtilmedi

- **Uygunluk değerlendirme yolu:** Article 32(3)

Bildirim süreleri

- **Erken uyarı (saat):** 24
- **Zafiyet bildirim süresi (saat):** 72
- **Zafiyet nihai rapor süresi (gün):** 14
- **Olay nihai raporu:** 1 ay
- **Resmî metin — bildirim alıcıları:** to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA

Destek süresi

- **Beyan edilen yıl:** 3.0
- **Asgari yıl:** 5
- **Uygun:** hayır
- **Not:** Beyan edilen destek süresi 3 yıl; md. 13(8) asgarisi 5 yıl. ASGARININ ALTINDA — ürün ömrü daha kısa değilse bu bir uygunsuzluktur.
- **Güncellemelerin erişilebilir kalacağı yıl:** 10

Tarihler

- **Genel uygulama tarihi:** 2027-12-11
- **Md. 14 bildirim yükümlülüğü:** 2026-09-11
- **Bölüm IV (onaylanmış kuruluşlar):** 2026-06-11
- **Resmî metin — uygulama tarihleri:** This Regulation shall apply from 11 December 2027. However, Article 14 shall apply from 11 September 2026 and Chapter IV (Articles 35 to 51) shall apply from 11 June 2026.
- **Kapsam notu:** CRA, AB pazarına sunulan DİJİTAL ÖĞELİ ÜRÜNLERE uygulanır (yazılım dahil). Üretici AB'de kurulu olmak zorunda değildir: ürün AB pazarına giriyorsa yükümlülük üretici, ithalatçı ve distribütör arasında paylaşılır. Bu yüzden Türkiye'de yerleşik bir yazılım üreticisi, ürününü AB'ye satıyorsa doğrudan kapsamdadır.

5. Hukuki dayanak ve kaynaklar

- **Hukuki dayanak:** Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 2, 13, 14, 31, 32 and 71, Annexes I, III, IV and VII; as amended by Regulation (EU) 2025/327 (EHDS)
- **Resmî Gazete (OJ) künyesi:** OJ L, 2024/2847, 20.11.2024
- **Resmî kaynak:** <http://data.europa.eu/eli/reg/2024/2847/oj>
- **Değişiklik zinciri:**
- Regulation (EU) 2025/327 (European Health Data Space)
- CELEX: 32025R0327
- Resmî Gazete (OJ) künyesi: OJ L, 2025/327, 5.3.2025
- Resmî kaynak: <http://data.europa.eu/eli/reg/2025/327/oj>
- Değişen: md. 13(4) ve md. 31(3): diğer AB mevzuatına da tabi ürünlerde TEK teknik dosya; md. 32(5a): EHR sistemi olarak sınıflanan ürünler Ek I uygunluğunu EHDS Bolum III prosedürüyle gösterir.

Sınır

Bu bir HAZIRLIK deęerlendirmesidir: CE iřareti, AB uygunluk beyanı ya da onaylanmış kuruluş incelemesi yerine gemez. Ürün sınıfı ve uygunluk yolu nihai olarak ürünün teknik özelliklerine göre belirlenir.

Nechh Robotics hukuk bürosu, akredite doęrulayıcı ya da onaylanmış kuruluş deęildir.

ÖRNEK · GEÇERSİZ RAPOR

ÖRNEK · GEÇERSİZ RAPOR

ÖRNEK · GEÇERSİZ RAPOR

ÖRNEK · GEÇERSİZ RAPOR