DG **DEPENDENCY GUARD · YÖNETİCİ GÜVENLİK ÖZETİ**

Rapor tarihi
8 Kas 2026 23:12

Örnek Mağaza API

Ortam **Üretim** · İnternete açık **Evet** · İş kritikliği **Yüksek**

⚠ **Öncelikli iş var**

4 konu öncelikli olarak ele alınmalı.

Aşağıdaki liste, önce ele alınması gereken konuları önem sırasıyla gösterir.

4 ⚠ Öncelikli · **0** Kontrol · **0** Planlı · **0** Bakım

NE TARANDI, NE BULUNDU?

Hazır paketler
Dış yazılım parçaları

✓ Tamamlandı · Kayıtlı sonuç
26 Eki 2026 16:20

1 paket, duyurulmuş açık kayıtlarıyla (OSV) karşılaştırıldı.
Saldırı bilgisi: KEV listesi 6 Kas 2026 (kayıtlı) · EPSS 7 Kas 2026 (kayıtlı).

5 bilinen açık · **1** etkilenen paket · **0** saldırıda kullanılan (KEV)

Açık kayıtlarının inceleme önceliği

Öncelikli **3** · Bilgi eksik **0** · Planlı **0** · Standart **2**

Projenin kendi kodu
Ekibin yazdığı JS/TS kodu

✓ Tamamlandı
8 Kas 2026 23:11

3 dosya, 3 hata türü için tarandı; adaylar otomatik incelendi.
Güvenlik haritası: 4 giriş noktası · kontrol: tamamlanan 9, aday 3.

3 kod adayı · **3** güçlü aday

Adayların otomatik inceleme sonucu

Güçlü **3** · Belirsiz **0** · Zayıf **0** · İncelenmedi **0**

ÖNCE NE YAPILMALI?

Sıralama: saldırıda kullanıldığı bilinen (KEV) açıklar → kritik paket açıkları → güçlü kod adayları → diğer öncelikli paketler → kontrol → planlı → bakım

1 ⚠ Öncelikli — **Sunucuda çalışan komutu güvenli hâle getirin**

Projenin kendi kodu · src/routes.js, satır 12 · CWE-78, dg.js.command-injection

Neden? Kullanıcıdan gelen veri, sunucuda çalıştırılan bir komuta ekleniyor (komut enjeksiyonu adayı). Otomatik inceleme bunu güçlü aday saydı.

Yapılacak: Komutu sabit tutun; kullanıcı verisini yalnızca doğrulanmış argüman olarak verin.

2 ⚠ Öncelikli — **Dosya okuma yolunu sınırlayın**

Projenin kendi kodu · src/routes.js, satır 21 · CWE-22, dg.js.path-traversal

Neden? Kullanıcıdan gelen veri, okunacak dosyanın yolunu belirliyor (dosya yolu aşımı adayı). Otomatik inceleme bunu güçlü aday saydı.

Yapılacak: Değeri izin verilen dosyalarla eşleyin; yolun izin verilen klasörde kaldığını doğrulayın.

3 ⚠ Öncelikli — **Veritabanı sorgusunu güvenli hâle getirin**

Projenin kendi kodu · src/routes.js, satır 32 · CWE-89, dg.js.sql-injection

Neden? Kullanıcıdan gelen veri, veritabanı sorgusunun içine doğrudan ekleniyor (SQL enjeksiyonu adayı). Otomatik inceleme bunu güçlü aday saydı.

Yapılacak: Sorguyu parametreli hâle getirin; kullanıcı verisini sorgu metnine eklemeyin.

4 ⚠ Öncelikli — **lodash paketini 4.18.0 veya üstüne güncelleyin**

Hazır paket · lodash 4.17.20 · CVE-2020-28500, CVE-2021-23337, CVE-2026-2950 +2

Neden? 5 bilinen güvenlik açığı var; en ciddisi yüksek önemde (CVSS 8,1). Önümüzdeki 30 günde istismar edilme olasılığı tahmini (EPSS) en yüksek %21,3. Proje üretimde veya kritik olarak işaretlendiği için öne alındı.

Yapılacak: Kaynaklara göre 4.18.0 sürümü bu açıkların tamamını kapatıyor; güncelleyip uygulamayı test edin.

BU RAPOR NEYİ GARANTİ ETMEZ?

⚠ **Bağımlılık bölümü, 26.10.2026 tarihli kayıtlı örnek sonuca dayanıyor (Açık içeren örnek · lodash 4.17.20); canlı tarama değildir, o tarihten sonra duyurulan açıklar görünmez.**

- Güvenlik garantisi veya sızma testi değildir; bulunmayan bir sorun, sorun olmadığı anlamına gelmez.
- Paketler yalnızca duyurulmuş açık kayıtlarıyla (OSV) karşılaştırıldı; henüz duyurulmamış açıklar görünmez.
- Kod analizi JS/TS dosyalarında üç hata türüyle sınırlıdır (komut, veritabanı sorgusu, dosya yolu); bulgular doğrulanmamış adaylardır.
- Öncelik bir inceleme sırasıdır. EPSS yalnızca olasılık tahminidir; KEV listesinde olmamak saldırıda kullanılmadığını göstermez. Ortam, internete açıklık ve kritiklik kullanıcının beyanıdır.

Terimler: Bağımlılık (hazır paket), projenin kullandığı ve başkalarının yazdığı hazır yazılım parçasıdır. **Bilinen açık**, herkese duyurulmuş güvenlik hatasıdır; çoğu CVE numarası taşır. **Kod adayı**, ekibin kendi kodundaki olası güvenlik hatasıdır; geliştirici doğrulamalıdır. **CVSS**, bir açığın teknik önemini 0–10 arasında gösteren puandır. **KEV**, ABD siber güvenlik ajansı CISA'nın gerçek saldırılarda kullanıldığı bilinen açıklar listesidir. **EPSS**, bir açığın önümüzdeki 30 günde istismar edilme olasılığına ilişkin günlük tahmindir.

Kayıtlar: bağımlılık taraması 08cc1e1f (kayıtlı örnek sonuç, canlı tarama 26 Eki 2026 16:20; OSV-Scanner 2.7.0; öncelik politikası 0.2.0, tarama anındaki proje bilgileri) · kaynak analizi b95e9db4 (8 Kas 2026 23:11; motor 0.3.0, kurallar 0.1.0; inceleme 3120d960, kural tabanlı ajan 0.1.0) · rapor 0.4.0. Rapor kayıtlardan her açılışta yeniden üretilir ve kayıtları değiştirmez; dil modeli kullanılmaz.