CERYVON BUSİNESS LOGİC & AUTHORİZATİON AUDİT

Sentetik Örnek Rapor

Modüller Arası Durum Tutarsızlığıyla Yinelenen İade

NexaFlow Commerce

Bu doküman yalnızca sentetik bir demonstrasyondur.

Herhangi bir gerçek şirkette güvenlik açığı bulunduğuna dair kanıt değildir.

Oluşturulma tarihi: 22 Haziran 2026

Yönetici Özeti

Bu sentetik örnekte teslim edilmiş bir sipariş için ilk iade tamamlandıktan sonra ödeme kayıtları iadenin tamamlandığını gösterir. CRM tarafındaki onaya uyumlu durum yeniden kullanılabilir kaldığında ikinci iade isteği final ödeme işlemine ulaşabilir.

Risk seviyesi	Uygulama	İş akışı
Yüksek	**NexaFlow Commerce**	**İade iş akışı**

Bu doküman yalnızca sentetik bir demonstrasyondur; herhangi bir gerçek şirkette güvenlik açığı bulunduğuna dair kanıt değildir.

Kapsam

Sentetik kapsam CRM, Order Management ve Payments modülleri arasındaki iade iş akışına odaklanır.

- CRM
- Order Management
- Payments
- İade iş akışı

Bulgu

Yüksek Risk

Etkilenen Akış

Teslim edilmiş sipariş için CRM onaylı ödeme iadesi

Beklenen Davranış

Final iade işlemi CRM onayını, sipariş iade uygunluğunu, ödeme ve iade durumunu, iade sayısını, tenant sınırını ve sipariş sahipliğini birlikte doğrulamalıdır.

Gözlenen Davranış

Final işlem, güvenlik açısından gerekli durum kontrollerinin yalnızca bir bölümünü doğruluyor.

Ön Koşullar

- Sipariş tenant_alpha kapsamındadır.
- Sipariş teslim edilmiş durumdadır.
- Order Management modülü iade uygunluğu ve sahiplik bağlamını yükler.
- CRM içinde destek iade talebi açılır ve CRM onayı kaydedilir.
- İlk iade ödeme modülünde tamamlanmıştır.
- CRM tarafında onaya uyumlu durum korunmuş veya yeniden kullanılmıştır.

Tekrar Üretim Zaman Çizelgesi

Adım	Aktör / Rol	Modül	Durum Geçişi	Sonuç
1	Destek	CRM	İade talebi açılır	CRM iş akışı başlar
2	Sistem	Order Management	Teslimat ve sahiplik bağlamı doğrulanır	Sipariş iade uygunluğu yüklenir
3	CRM	CRM	Onay kaydedilir	İade için onaya uyumlu durum oluşur
4	Sistem	Payments	İlk iade işlenir	Ödeme iade edilmiş duruma geçer
5	Destek	Payments	İkinci iade isteği final işleme ulaşır	Kontrol kapsamı eksik kalır
6	Sistem	Payments	İade sayısı ikinci kez artar	Yinelenen iade koşulu oluşur

Tekrar Üretim Adımları

1. Destek temsilcisi CRM üzerinden teslim edilmiş sipariş için iade talebi açar.
2. Order Management modülü siparişin teslim edildiğini, tenant bağlamını ve iade uygunluğunu yükler.
3. CRM iş akışında iade onayı kaydedilir.
4. Payments modülü ilk iadeyi işler ve ödeme durumunu iade edilmiş olarak günceller.
5. CRM onayıyla uyumlu durum korunurken ikinci iade isteği hazırlanır.
6. İkinci istek final iade işlemine ulaşır ve iade sayısı ikinci kez artar.

Kanıt

Doğrulanan Kontrol

- CRM onay durumu

Eksik veya Yetersiz Kontrol

- Sipariş için daha önce gerçekleştirilen iade sayısı
- Ödeme işleminin mevcut durumu
- İadenin daha önce tamamlanıp tamamlanmadığı
- Sipariş sahipliği
- Tenant sınırı
- Sipariş iade uygunluğu

Sentetik modelde final işlem 1 kontrolü doğrularken 6 gerekli kontrol eksik kalır. İkinci final iade adımından sonra iade sayısı 2 olur.

Zayıf Kontrol Alanları

- Sipariş için daha önce gerçekleştirilen iade sayısı
- Ödeme işleminin mevcut durumu
- İadenin daha önce tamamlanıp tamamlanmadığı
- Sipariş sahipliği
- Tenant sınırı
- Sipariş iade uygunluğu

İş Etkisi

- Aynı sipariş için ikinci iade nedeniyle doğrudan finansal kayıp
- CRM, sipariş ve ödeme kayıtları arasında tutarsızlık
- Mutabakat ve operasyon ekipleri için ek inceleme yükü
- Denetim izi bütünlüğü ve olay takibi riski

Düzeltme Önerileri

- Final iade işleminde CRM, sipariş ve ödeme durumunu tek bir sunucu tarafı guard ile doğrulayın.
- İade oluşturma, ödeme durumu güncelleme ve denetim kaydını atomik işlem sınırı içinde yürütün.
- Sipariş veya ödeme referansı bazında idempotency uygulayın.
- Daha önce tamamlanmış iade, iade edilmiş ödeme durumu veya sıfırdan büyük iade sayısı varsa ikinci iadeyi reddedin.
- Her final işlemde tenant sınırını ve sipariş sahipliğini yeniden doğrulayın.
- Durum geçişlerini merkezi bir servis üzerinden yönetin.
- Şüpheli tekrar iade denemeleri için denetim kaydı ve uyarı üretin.

Yeniden Test Rehberi

- İlk iade tamamlandıktan sonra aynı sipariş için ikinci iade isteğini deneyin.
- CRM onayı korunurken ödeme durumu iade edilmiş olduğunda final işlemin reddedildiğini doğrulayın.
- Farklı tenant bağlamından gelen isteğin reddedildiğini doğrulayın.
- Aynı sipariş veya ödeme referansı tekrarlandığında ikinci finansal işlem oluşmadığını kontrol edin.

Yöntem ve Sınırlamalar

Ceryvon değerlendirmesi yetkili ortamlarda, belirli iş akışlarına odaklanır. Bu örnek tüm güvenlik açıklarının bulunacağını veya eksiksiz güvenlik kapsamı sağlandığını iddia etmez.

- Yalnızca yetkili ortamlar ve onaylanmış kapsamlar içinde uygulanır.
- Belirli iş akışlarına odaklanan analizdir.
- Tüm güvenlik açıklarının bulunacağını garanti etmez.
- Bu çıktı sentetik demonstrasyon amacıyla hazırlanmıştır.