

Management Report

Nori API Security Assessment

Nori | API: REST

PREPARED FOR	Nori
PROJECT	Nori API Security Assessment
AUTHOR	Palisade Security
DATE	2024-09-07
VERSION	1.1

Executive Assessment

Overall risk: **CRITICAL**

Nori API supports a live multi-tenant invoicing service. The assessment supports ISO/IEC 27001 compliance preparation and production risk reduction. Testing covered user provisioning, invoices, customer records, exports and administrative error handling using approved test tenants and controlled records. The assessment identified five findings: one Critical, one High, two Medium and one Low. Unauthenticated account creation grants tenant-administrator access, and invoice operations fail to enforce tenant boundaries. Contain these exposures immediately and prioritize production fixes.

Risk applies to the assessed production API and tested tenant roles. Demonstrated account-provisioning and tenant-isolation failures expose the live service. Validation used controlled records in approved test tenants; conclusions do not extend to unrelated systems.

- Contain the Critical exposure immediately and prioritize production fixes.
- Assign owners and fund a focused remediation sprint.
- Retest authorization and data-delivery controls before accepting residual risk.

FINDINGS

Finding Severity

Counts represent unique findings.



RISK

Priority Findings

Unauthenticated admin creation An attacker can take over a tenant's invoices, customer data and user access. Recommended action: Validate single-use invitations. Assign tenant and role on the server, not from request fields.	CRITICAL
Cross-tenant invoice access Customers can access another tenant's invoices or tamper with payment references. Recommended action: Enforce tenant-scoped lookups and a shared object policy on every invoice read and update.	HIGH

Decision and Next Steps

ACTIVITY	DESCRIPTION	PRIORITY	OWNER
Contain live exposure	Restrict account creation within 24 hours and fix tenant isolation within 7 days. Identity and Billing teams own the changes; verify the deployed fixes with a controlled production retest.	Immediate	Engineering lead
Close data-exposure gaps	Within 30 days, enforce export revocation and minimize customer responses. Retest existing links and member/admin response differences.	Short Term	Data services and Customer platform
Complete hardening	Within 60 days, replace verbose admin errors with stable error responses. Retain detailed diagnostics in restricted logs.	Medium Term	Platform team
Record closure evidence	Use negative and positive regression cases, verify persisted state, and record explicit risk acceptance for any deferred item.	Short Term	Security lead

Report Details

APPLICATION / ENVIRONMENT	Nori API / production
TESTING WINDOW	2024-08-31 to 2024-09-04
ASSESSED RELEASE	Not recorded
SCOPE	Ten production REST API routes at api.nori.example/v1, using two approved test tenants.
SCOPE EXCLUSIONS	Unrelated customer tenants and records, payment processing, third-party providers, source-code review, infrastructure exploitation, and destructive, denial-of-service or load testing.
DOCUMENT	Version 1.1
AUTHOR	Palisade Security