

Remediation Summary

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

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

FINDINGS

Finding Severity

Counts represent unique findings.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
1	1	2	1	0

SUMMARY VISUALS

Remediation Tracker

Remediation targets are proposed unless explicitly agreed. Finding status and retest outcome are recorded separately.

FINDING	ACTION AND VERIFICATION	OWNER / TARGET	STATUS
F-01 Unauthenticated admin creation Critical	Validate single-use invitations. Assign tenant and role on the server, not from request fields. Acceptance criteria No invitation means no account or token. Approved invitations grant only the assigned role.	Identity team P0 - immediate Within 24 hours Proposed from 2024-09-07	Open Not retested
F-02 Cross-tenant invoice access High	Enforce tenant-scoped lookups and a shared object policy on every invoice read and update. Acceptance criteria Cross-tenant requests fail without changing data; authorized own-tenant requests succeed.	Billing team P1 - urgent Within 7 days Proposed from 2024-09-07	Open Not retested

FINDING	ACTION AND VERIFICATION	OWNER / TARGET	STATUS
F-03 Revoked exports remain accessible Medium	Check revocation and expiry on every download and invalidate cached delivery when access is withdrawn. Acceptance criteria Revoked links fail from fresh clients and caches. Valid links expire as configured.	Data services P2 - next release Within 30 days Proposed from 2024-09-07	Open Not retested
F-04 Excess customer data Medium	Use explicit, role-aware response schemas and test forbidden fields in nested and bulk responses. Acceptance criteria Member responses omit both restricted fields; administrator responses retain them.	Customer platform P2 - next release Within 30 days Proposed from 2024-09-07	Open Not retested
F-05 Verbose admin errors Low	Validate input, return non-sensitive errors, and keep detailed diagnostics in restricted logs. Acceptance criteria Malformed input returns 422 without exception or schema details.	Platform team P3 - hardening Within 60 days Proposed from 2024-09-07	Open Not retested