

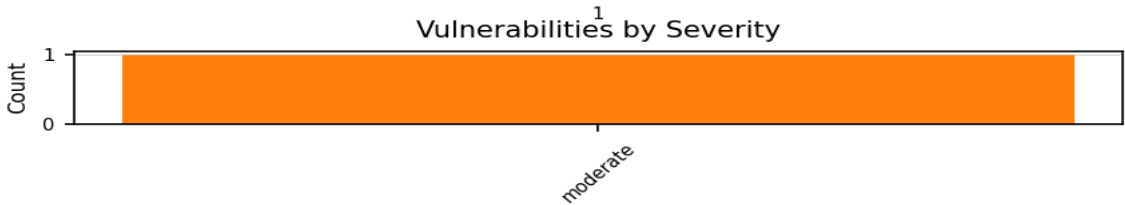
TuneSpace-FE — Compliance & Vulnerability Report

Compliance Score: 92.0%

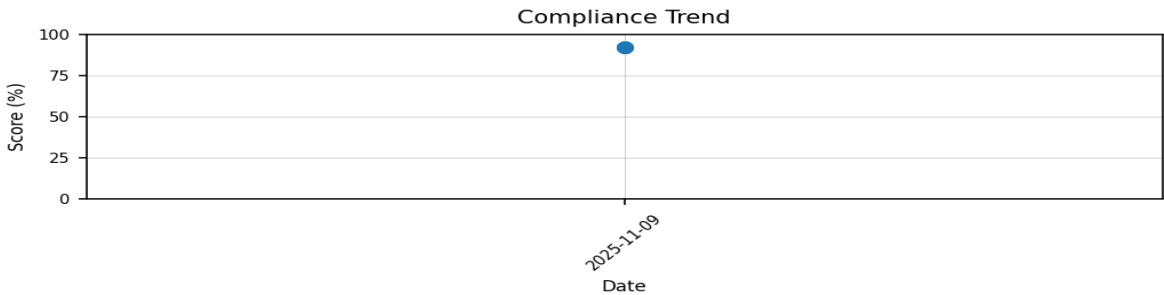
Standards Compliance

Standard	Status
ISO_27001	Compliant
NIST_SP_800_53	Compliant
OWASP	Compliant

Vulnerability Distribution



Compliance Trend



Detailed Control Scores

A.8.9 — Configuration management (*Technological*) — 90.0%

Summary Improper or inconsistent configuration management can lead to vulnerabilities, exposing systems to unauthorized access, data breaches, and operational disruptions. Effective configuration management ensures that systems remain secure and compliant with organizational policies and standards. **Remediation Steps** **Establish a Configuration Management Policy** Define and document the accepted configurations for systems and applications within your organization. **Implement Automated Configuration Management Tools** Use tools like Ansible, Chef, or Puppet to automate the deployment and monitoring of configurations. Example Command: `ansible-playbook playbook.yml` (assuming you're using Ansible for configuration management). **Regularly Review and Update Configurations** Schedule periodic audits of system configurations to ensure they align with your established policy. **Guidance:** Utilize tools like CIS-CAT to assess system compliance against established benchmarks. ■ Support this free API: https://www.paypal.com/donate/?hosted_button_id=XS3CAYT8LE2BL

Vulnerability Detail Summary

Component	Version	Vuln ID	Severity	Fix / Recommendation
vite	7.1.3	GHSA-93m4-6634-74q7	Medium	Update to: 5.4.21