MyESI Automated Compliance & Vulnerability Assessment

Project: myesi-risk-service

Generated: 2025-11-12 15:21 UTC **User:** 1

1. Executive Summary

- Compliance Score: **60.0%**
- Average Risk Score: **10.00**
- Total Vulnerabilities: **4**

Standards Compliance:

Standard	Status
ISO_27001	Partially
NIST_SP_800_53	Needs Review
OWASP	Needs Review

2. Compliance Controls Overview

critical — *(General)* — Score: **50.0%**

1 Plan fix in next release cycle. Limit exposure through configuration hardening.
2 Validate compliance and re-run assessment.

3. Vulnerability Findings

#	Component	Version	Vuln ID	Severity	Fix / Recommendation
1	**pydantic**	2.12.3	MAL-2025-4867	**Critical**	### Summary This control requires attention in General. ### Remediation Steps - Immediately patch or isolate affected components. Deploy emergency fixes and block exploit paths. - Validate compliance and re-run assessment.
2	**python-dotenv**	1.2.1	MAL-2025-48037	**Critical**	### Summary This control requires attention in General. ### Remediation Steps - Immediately patch or isolate affected components. Deploy emergency fixes and block exploit paths. - Validate compliance and re-run assessment.
3	**typing-extensions**	4.15.0	MAL-2025-47895	**Critical**	### Summary This control requires attention in General. ### Remediation Steps - Immediately patch or isolate affected components. Deploy emergency fixes and block exploit paths. - Validate compliance and re-run assessment.
4	**uvicorn**	0.38.0	MAL-2025-4901	**Critical**	### Summary This control requires attention in General. ### Remediation Steps - Immediately patch or isolate affected components. Deploy emergency fixes and block exploit paths. - Validate compliance and re-run assessment.

4. Code Findings (Static Analysis)

1. dockerfile.security.missing-user.missing-user (Error / MEDIUM)

/app/tmp/repos/semgrep-20251112111552/Dockerfile
By not specifying a USER, a program in the container may run as 'root'. This is a security hazard. If an attacker can control a process running as root, they may have control over the container. Ensure that the last USER in a Dockerfile is a USER other than 'root'.

```
CMD ["uvicorn", "app.main:app", "--host", "0.0.0.0", "--port", "8004", "--reload"]
```

https://owasp.org/Top10/A04_2021-Insecure_Design

Suggested Fix:

Summary This control requires attention in security. Remediation Steps Investigate severity and verify exploitability before mitigation planning. Validate compliance and re-run assessment.

Generated by MyESI on 2025-11-12 15:21 UTC — User: 1