

Evidence Review

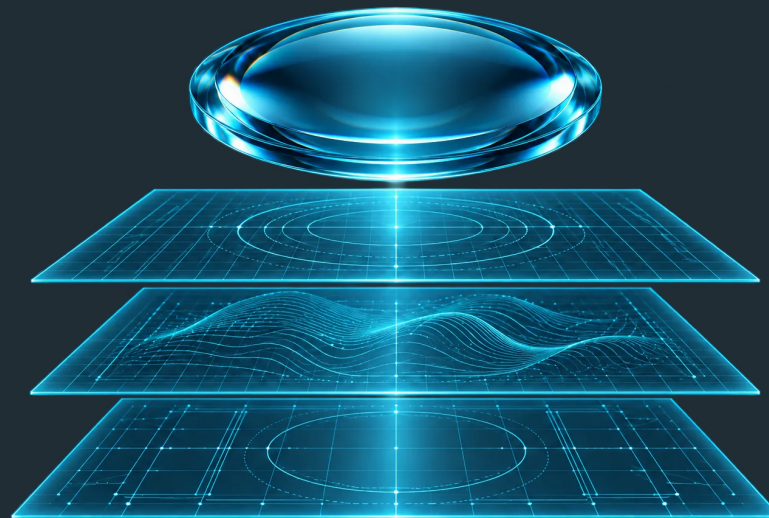
Montclair Digital

01 September 2026 - 05 September 2026

Prepared by Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL



Engagement scope

Two namespaces, eight workload manifests, associated service accounts and namespace policies.
Read-only review of exported desired-state and running-state records; host access, denial-of-service tests and provider control plane excluded.

Architecture and trust boundaries

Private image registry -> managed staging cluster -> orders and billing namespaces. Application ingress is encrypted. The provider-managed control plane and underlying hosts are excluded.

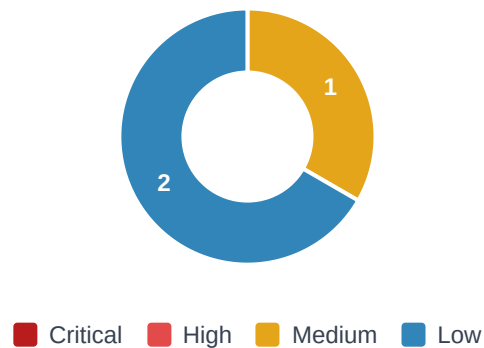
Coverage and limitations

Eight workload manifests and two namespace-policy records reviewed. E-01 covers resource budgets, E-02 runtime identities and E-03 service-account usage. Host and provider-control-plane testing were excluded.

Findings overview

Finding	Severity	CVSS v3.1
F-1 / Workloads have no effective resource limits	Low	3.3 / 10
F-2 / Application workloads run as the root user	Medium	Not applicable
F-3 / Unused service-account tokens are mounted into workloads	Low	Not applicable

Risk distribution



Priority finding

F-1

Low / CVSS 3.3 / 10

F-1 affects five of eight workloads. Define effective resource budgets and confirm normal and peak behavior before enforcing the agreed limits.

Evidence and observation

Observation record	Evidence and context															
Finding reference / evidence ID Expected behavior, observed behavior, date and version.	E-01: five workload records omit resource limits; the two namespace records do not provide defaults. <table><tr><th colspan="3">E-01 / KUBERNETES SECURITY</th></tr><tr><th>Reviewed item</th><th>Scope</th><th>Recorded state</th></tr><tr><td>Workload sample</td><td>8 workloads</td><td>5 without effective limits</td></tr><tr><td>Namespace sample</td><td>orders / billing</td><td>No equivalent default limits</td></tr><tr><td colspan="3">Evidence register / Review window: 01-05 September 2026</td></tr></table> E-01 - Reviewed record extract, September 2026.	E-01 / KUBERNETES SECURITY			Reviewed item	Scope	Recorded state	Workload sample	8 workloads	5 without effective limits	Namespace sample	orders / billing	No equivalent default limits	Evidence register / Review window: 01-05 September 2026		
E-01 / KUBERNETES SECURITY																
Reviewed item	Scope	Recorded state														
Workload sample	8 workloads	5 without effective limits														
Namespace sample	orders / billing	No equivalent default limits														
Evidence register / Review window: 01-05 September 2026																

Correction and acceptance criteria

Platform engineering will define requests and limits with application owners. Closure requires all eight workloads to have approved budgets and a successful representative non-production test.

Correction	Retest result
Workload hardening / platform engineering	Not retested at issue

Shared causes

The service onboarding checklist does not require a completed runtime-hardening review. Introduce an owner-approved check covering resource budgets, runtime identity and API credential requirements.

Dependencies and rollout

Application owners must provide representative workloads and permission requirements. Roll out changes in staging, retain the prior manifest and document rollback ownership before wider adoption.

Action plan

F-1: platform lead, 30 September. F-2/F-3: application and platform leads, 16 October. All Open. Preserve the reviewed manifests and regression results as closure evidence.

Owner	Target	Closure evidence
Lina Bernard, platform lead	30 Sep-16 Oct 2026 (planned)	Approved manifests and successful regression checks

Retest scope

Proposed 19-20 October 2026 on the corrected staging release. Verify all eight workloads, their effective identities and credential dependencies. No retest result is available at issue.

Open decisions

Lina Bernard owns implementation; Sophie Roux reviews closure evidence. Confirm the maintenance window and regression capacity at the 23 September review. No finding is accepted or closed in this issue.