PUBLIC DEMO / SYNTHETIC DATA ONLY

From synthetic CVE to reviewable evidence

Case CM-DEMO-2026-0042 | Example Product Company | Checkout API | Generated 2026-08-13 14:30 UTC

96 / 100	**Priority**	**24 hours**	**Recommended action window**

Decision summary

A synthetic critical vulnerability observation is present in the immutable image currently running the Checkout API. The workload is reachable through a public ingress and belongs to a mission-critical payment path. CyberMeasures recommends owner confirmation and replacement of the affected image within 24 hours.

This package demonstrates evidence preparation. The identifier, company, assets, hashes, addresses and people are fictitious. It does not determine CRA reportability.

Evidence chain

STEP	OBSERVED FACT	SOURCE	TIME
Vulnerability	DEMO-CVE-2026-0042; critical; fixed in 4.2.7	Synthetic scanner	14:22
Image	checkout-api@sha256:8d2e...c014	SBOM / scan	14:22
Runtime	deployment/checkout-api; 6/6 replicas	Kubernetes API	14:23
Product	Mission-critical; owner Platform Security	Product register	14:24
Exposure	Public TLS ingress on TCP 443	Ingress API	14:23
Traffic	Connections observed from the public edge	Synthetic flow summary	14:25
Priority	96/100 with visible component scores	CyberMeasures policy	14:26
Decision	Replace image; validate rollout; preserve evidence	Security reviewer	14:30

PRIORITY AND ACTION

Why this finding is first

The score is explainable. No hidden model is allowed to convert missing context into false confidence.

FACTOR	SCORE	EVIDENCE
Vulnerability severity	40 / 40	Synthetic scanner severity is critical.
Runtime presence	20 / 20	The immutable digest is active in six replicas.
Exposure	20 / 20	A public TLS ingress routes to the workload.
Business criticality	16 / 20	Product register marks the path mission-critical and names an owner.
TOTAL	96 / 100	Remediate before lower-context scanner findings.

Recommended action

01 Platform Security confirms the affected package and available fixed image.

02 Service owner deploys version 4.2.7 or a vendor-approved mitigation.

03 Operator verifies the old digest is no longer active or externally reachable.

04 Security reruns the scanner and evidence collection.

05 Legal or compliance independently determines whether CRA reporting criteria are met.

Evidence minimization

Raw packet payloads, secrets and customer log bodies are excluded. Each displayed fact has a named source and observation time. The package keeps explicit limitations next to supporting evidence, and reviewer sign-off remains separate from automated priority.

REVIEW AND LIMITATIONS

A decision record, not a compliance claim

ROLE	DECISION	TIME	NOTE
Platform Security	Remediate within 24 hours	14:30	Public critical workload
Service owner	Replacement accepted	14:36	Change window opened
Compliance owner	Reportability review required	14:42	Legal determination outside CyberMeasures

What this package proves

A reviewer can follow the vulnerability to immutable image, active workload, public exposure, product owner, priority and proposed action. Each material statement is connected to its source and observation time.

What it does not prove

This synthetic package is not a vulnerability disclosure, incident report, legal opinion, conformity assessment or proof that reporting is required. Production use depends on authorized customer sources, retention, reviewers and reporting procedures.

Ready to test your evidence path? **hello@cybermeasures.io**