

INTELLIGENCE, MADE ACCOUNTABLE.

SECURITY ASSURANCE REPORT

ASTER VALE FINANCIAL / ILLUSTRATIVE ASSESSMENT

2026

PREPARED FOR

The board. The CISO. The people fixing it.

EDITION / 22 SEPTEMBER

Public sample · fictional organization
No live customer assessment.

A report you can interrogate.

Every conclusion should lead back to an observation. Every observation should carry a boundary. Every open issue should have a route to closure.

Document control

Reference

Organization

Illustrated assessment window

Illustrated retest / issue

Distribution

Assessment status

This edition

DS-AVF-2026-09 · version 1.0

Aster Vale Financial — entirely fictional

14–18 September 2026

21 September / 22 September 2026

Public sample. No customer information.

Designed example; no live tests were performed.

What this demonstrates

A proposed reporting standard: executive decisions, scoped technical evidence, remediation verification and a traceable record of activity. All findings, observations, roles and dates inside the case are synthetic.

What it does not establish

This sample is not a security opinion on any real organization, an ISO certification, an independent audit or evidence that Decima has completed a customer engagement.

One assessment. Three reading paths.

01

Board / 4–6

Exposure, decisions and accountable owners.

02

Security / 7–29

Scope, attack paths, evidence and closure.

03

Assurance / 30–37

Control context, audit trail and limitations.

Inside this edition	Pages
Executive position and decisions	04–06
Scope, authorization and test coverage	07–10
Attack paths and observed defenses	11–14
Findings register and 12 detailed records	15–27
Remediation plan and retest outcomes	28–29
ISO, NIST and testing crosswalks	30–31
Audit design, detection and testing cadence	32–34
Limits, evidence ledger and sources	35–37

The same evidence serves all three readers. Presentation changes; the underlying record does not.

Protect the boundary. Then prove the fix.

In this fictional estate, the most consequential weaknesses sit at three trust boundaries: report access, payout-event authenticity and build-to-production identity.

12

CONFIRMED FINDINGS

04

VERIFIED FIXED

08

STILL OPEN

What requires attention now

Disable the unsafe report-export path and reject unauthenticated payout events before the next release. F01 and F02 remain open critical issues. The build identity issue, F03, is closed only for the exact policy and workflow retested.

What is working

Privileged sign-in enforcement, one protected tenant endpoint and constrained network routes stopped their tested scenarios. Those results are valuable evidence about specific controls; they do not establish that the entire estate is secure.

MANAGEMENT POSITION

Contain the two open critical paths now. Schedule the remaining six open findings by owner, and require evidence of retest before closure.

Four decisions. Named accountability.

01 **Contain report exposure**

Disable unauthenticated export access. Restore it only after tenant-pair read and update tests pass.

HEAD OF APPLICATION ENGINEERING / 23 SEP / F01

02 **Protect payout state**

Reject unverified provider events. Keep the dry-run regression suite as a release gate.

PAYMENTS ENGINEERING LEAD / 23 SEP / F02

03 **Fund the closure cycle**

Reserve engineering capacity for tenant authorization and immediate privilege revocation, followed by independent retest.

CISO + ENGINEERING LEADERSHIP / 06 OCT / F04-F05

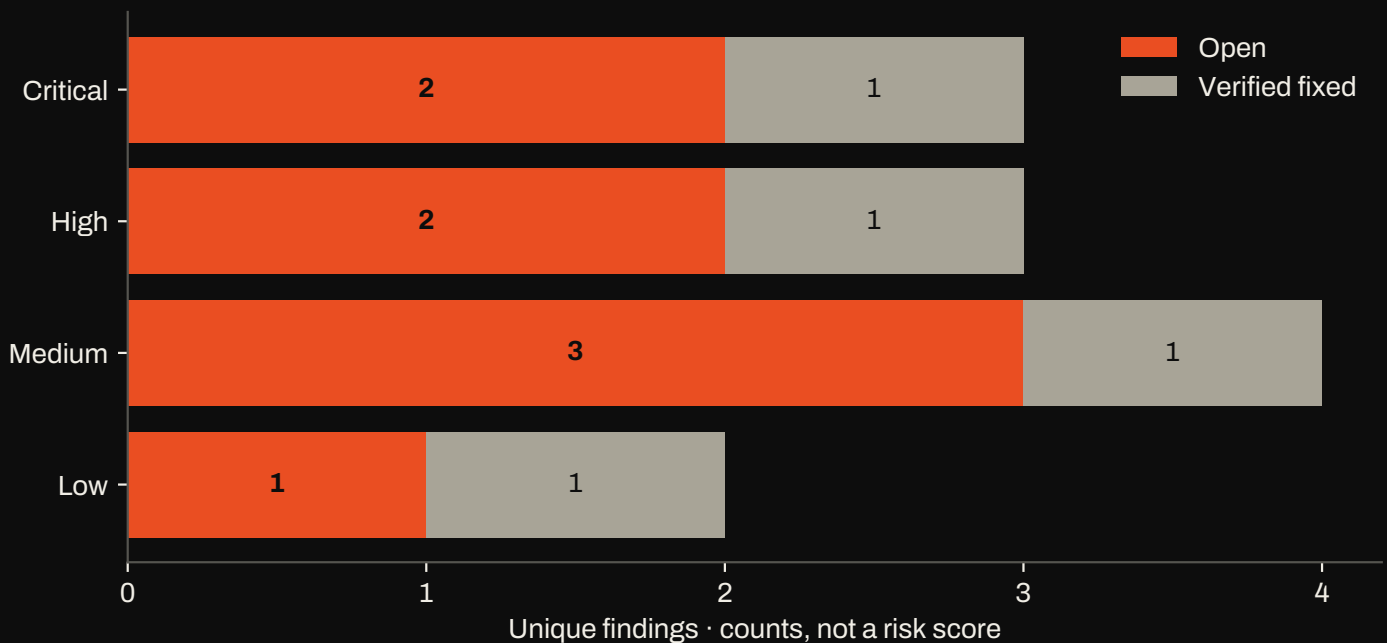
04 **Assign residual-risk authority**

Approve any exception explicitly, with expiry, scope, compensating control and a recorded business reason.

EXECUTIVE RISK OWNER / BEFORE AN OVERDUE ISSUE IS ACCEPTED

Count what matters.

Finding severity and closure status describe different things. A fixed critical issue remains part of the historical record; it leaves the open remediation queue.



How to read the ratings

Eleven technical findings use CVSS v3.1 base vectors. F10 is a qualitative control observation. Business urgency also considers transaction integrity, tenant separation and privileged access; it is not derived from a scanner score alone.

No invented precision

This report assigns no probability of breach, dollar loss or organization-wide security score. The evidence does not support those estimates. An open finding count is a work queue, not an actuarial forecast.

OPEN: 2 CRITICAL / 2 HIGH / 3 MEDIUM / 1 LOW

The estate in view.

46

NAMED ASSETS

06

BUSINESS SERVICES

03

TEST USER ROLES

Business service

- Merchant portal
- Payout processing
- Partner connectors
- Operator access
- Build and release
- Recovery and telemetry

Included boundary

- Public app + export worker
- API + dry-run event handler
- Fetch worker + test sink
- Console + session service
- CI identity + two cloud accounts
- Seeded backup + event pipeline

Primary concern

- Tenant confidentiality
- Ledger integrity
- Internal reachability
- Privileged access
- Production separation
- Restore access / attribution

External / 18 assets

Public gateways, named web applications, API routes and approved storage endpoints. The 18 external assets are included in the total of 46, not added to it.

Internal / 28 assets

Application services, identities and control-plane resources reached through the approved connector. No discovery result automatically expands authorization.

ALL HOSTNAMES USE THE RESERVED .EXAMPLE NAMESPACE.

Permission is a technical boundary.

Ownership verification, signed authority and an enforced scope are separate requirements. Possession of a domain does not automatically authorize testing its suppliers or every service behind it.

01 / Verify ownership

Use a DNS challenge or an approved domain connector. Record the verified domain, evidence, actor and time. Identify shared hosting and third-party services before tests are enabled.

02 / Approve the engagement

An authorized executive signs the rules of engagement: assets, techniques, windows, data handling, stop conditions and emergency contacts. Record the exact signed scope revision.

03 / Enforce the scope

Resolve and re-check destinations at execution time. The worker enforces allowed assets, rate limits and tool permissions outside the model. A redirect does not grant new authority.

04 / Stop and preserve

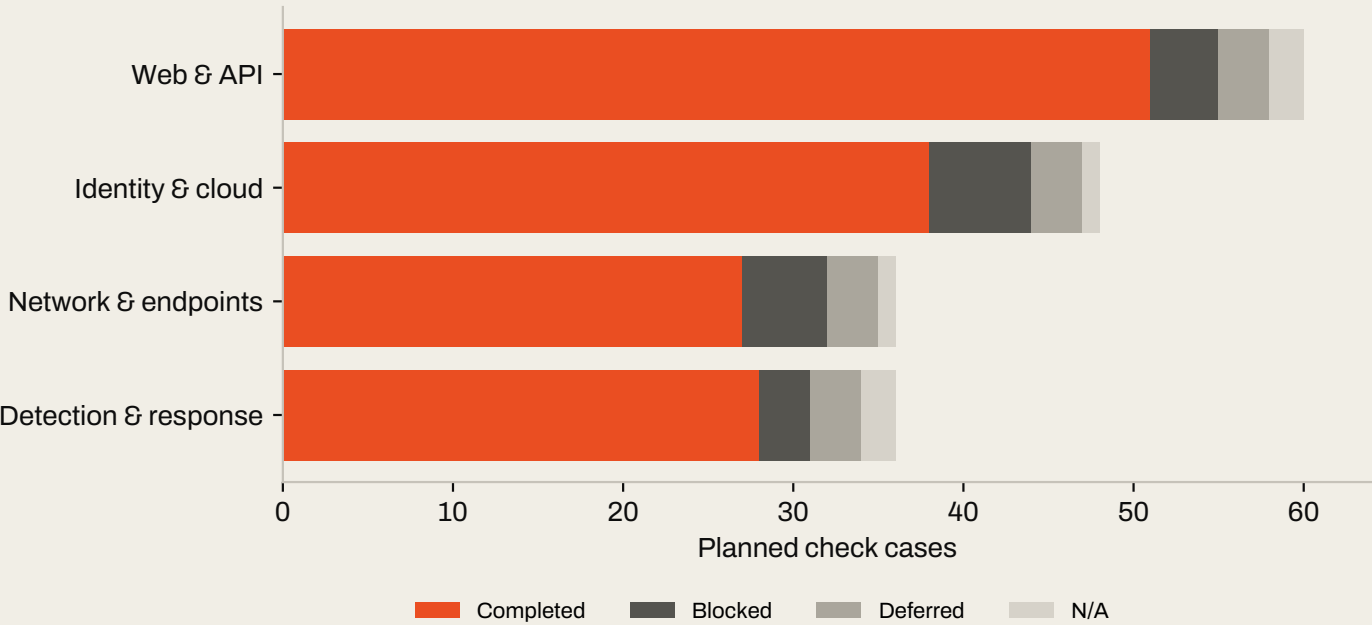
Halt on service instability, unexpected sensitive data or a customer stop request. Preserve the action record, notify the engagement contact and require approval for a material scope change.

EXCLUDED IN THIS SAMPLE

Live payment movement, destructive tests, social engineering, persistence, denial of service, real personal data and unapproved third-party infrastructure.

Show the blind spots.

144 of 180 planned check cases completed: 80% of the original plan. The remaining cases stay visible, including six that did not apply to the agreed estate.



State	Count	What it means
Completed	144	An outcome was recorded; this does not mean every check passed.
Blocked	18	Required access or an approved test dependency was unavailable.
Deferred	12	Moved outside the time or cost envelope; still requires a decision.
Not applicable	6	A documented scope condition made the case irrelevant.

Priority gap: the recovery drill and secondary identity provider were not fully exercised. Neither receives a positive assurance conclusion.

From signal to defensible finding.

A model can propose a hypothesis. A finding needs a reproducible observation, a bounded impact statement and review. This sample illustrates that workflow; it is not an executed model benchmark.

01	Collect	Record scoped asset identity, configuration and run context before interpreting output.
02	Challenge	Exercise the hypothesis with an approved, minimally disruptive check and a useful negative control.
03	Correlate	Join observations by asset, identity and run. Preserve separate failure causes; merge genuine duplicates.
04	Review	Validate the reasoning, severity assumptions and claimed impact. Keep unconfirmed leads out of the confirmed register.
05	Retest	Repeat the original failure case after the fix, plus a legitimate positive control. Preserve both states.

64 candidate signals → 12 confirmed findings; 38 dismissed or duplicate; 10 unconfirmed; 4 outside scope. Unconfirmed and excluded items are not evidence of a vulnerability.

One missing check. A crossed boundary.

Report delivery path / F01 / Open critical

UNAUTHENTICATED CALLER

No session or tenant membership



EXPORT REFERENCE

Caller-supplied object locator



REPORT WORKER

Missing object authorization



SOUTH TENANT REPORT

Seeded data read + destination changed

The line represents a demonstrated synthetic sequence. It does not imply lateral movement to a database, a full tenant dump or compromise of the wider network.

Where the proof stops.

Step	Observation	Evidence
Entry	Anonymous request reached the export handler.	EV-F01
Read	South report marker returned without tenant membership.	EV-F01
Integrity	Delivery destination changed to an approved sink.	EV-F01
Control	Same-tenant permitted flow remains a required retest check.	Pending
Stop	No bulk export, record enumeration or real email delivery.	Scope boundary

Attack-chain interpretation

The missing access check is sufficient to explain both observed effects. The report does not inflate one root cause into separate critical findings for each response. F04 remains separate because it concerns a different authenticated API and enforcement path.

Closure must break the path

A login screen alone is insufficient. Authorization must bind the authenticated principal to the requested report at the server-side operation boundary. Destination updates need their own explicit permission check.

EVIDENCE QUESTION FOR A REVIEWER

Can another assessor reproduce the unauthorized operation from this record, and can they tell precisely which additional effects were never attempted?

A build is not a production identity.

F03 / Original path closed in the retest fixture

01 TEST BRANCH

Valid workload token; no protected release approval

02 TRUST POLICY

Repository matched; environment and branch omitted

03 PRODUCTION ROLE

Read, deployment change and service-disable permissions

RETEST / 21 SEPTEMBER

Unprotected branch denied. Approved release allowed with reduced permissions.

Residual limit: other repositories and cloud accounts require their own effective-permission review. One closed path is not proof that every production identity is constrained.

Credit the controls that held.

A useful assessment records resistance as carefully as exposure. These are positive outcomes for named scenarios, with their limits attached.

Control exercised	Observed result	Limit
Privileged sign-in	Unenrolled operator could not complete the required second factor.	Recovery and alternate identity provider incomplete.
Adjacent tenant API	Cross-tenant request rejected at the server-side membership check.	One handler; F04 shows inconsistent coverage.
Worker egress boundary	Direct route to a disallowed test segment was blocked.	Connector redirect path still failed in F07.
Backup write policy	Anonymous writes and listing were denied.	Read exposure remained until F06 was fixed.
Approved release path	Protected workflow still deployed after the F03 fix.	Only the seeded service and role were retested.

INTERPRETATION

“Blocked in this scenario” is a supported conclusion. “Cannot be bypassed” requires evidence this limited assessment does not provide.

The complete work queue.

As of the 21 September retest. Historic severity is preserved after closure. Proposed due dates are illustrative management targets.

ID	Finding	Severity	CVSS	State
F01	Report export authorization	Critical	9.1	Open
F02	Payout event authenticity	Critical	9.1	Open
F03	Build-to-production identity	Critical	9.9	Fixed
F04	Invoice tenant authorization	High	8.1	Open
F05	Operator session revocation	High	8.1	Open
F06	Public backup read	High	7.5	Fixed
F07	Connector internal fetch	Medium	6.5	Open
F08	Private response caching	Medium	5.3	Fixed
F09	Payout replay control	Medium	6.5	Open
F10	Administrative audit gap	Medium	—	Open
F11	Legacy TLS configuration	Low	3.7	Fixed
F12	Verbose diagnostics	Low	3.1	Open

F10 is a qualitative control observation with no CVSS base score. “Fixed” means the defined retest passed in the fixture, not that the wider control was certified.

Report exports bypass tenant isolation

CRITICAL / OPEN

CVSS 9.1

exports.astervale.example

Business impact

An unauthenticated party could read a different tenant's financial reports and replace an export's delivery destination. Exposure concerns both confidential merchant information and the integrity of reporting workflows.

Observed behavior

In the synthetic tenant pair North and South, the report service accepted an export reference without a session. A request for South's seeded report returned its marker to the North test context. A second request changed the destination to a controlled sink. Two independent repetitions produced the same result.

Why it happens

The export worker trusted the reference carried in the request. Neither the read handler nor the destination-update handler resolved the reference against an authenticated tenant membership.

Limits of the evidence

Only two seeded reports and a sink address were used. The scenario does not establish how many customer records would be reachable, whether references are enumerable at scale, or whether historic data was accessed.

Required correction

Require authentication on every export operation. Resolve tenant identity server-side, bind every object lookup to that tenant, and separately authorize destination changes. Make links short-lived and single-purpose; treat an opaque identifier as a locator, never as permission.

What closes the finding

Repeat the original read and update requests without a session and with the wrong tenant. Both must fail without leaking object existence. Verify permitted same-tenant access still works and confirm the denied attempts appear in the audit stream.

anonymous read: 200 / seeded marker SOUTH-04; destination update: accepted

HEAD OF APPLICATION ENGINEERING / 23 SEP

Evidence EV-F01 · CWE-862 · ISO Annex A context 8.3 / 8.26 / 8.29

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Payout events accept an unverified sender

CRITICAL / OPEN

CVSS 9.1

payouts.astervale.example

Business impact

A forged settlement event could alter payout state and obstruct legitimate processing. The critical rating reflects demonstrated integrity and availability effects in the payout simulator, not a claim that money was stolen.

Observed behavior

An unsigned event reached the same state-transition handler as a signed provider event. In the isolated simulator it marked a seeded payout as settled and prevented the legitimate event from completing the expected transition. The event carried no valid provider authentication.

Why it happens

The gateway checked JSON shape and source metadata but did not authenticate the event body. Trust was established from caller-controlled fields before business state was changed.

Limits of the evidence

All effects were confined to a dry-run payout ledger. No bank, processor or live settlement network was contacted. Whether the production provider offers a particular signing mechanism must be confirmed before implementation.

Required correction

Authenticate the exact raw body using the provider's documented mechanism before parsing or state mutation. Enforce timestamp tolerance, reject missing authentication, support controlled key rotation and fail closed. Keep event authenticity separate from replay protection in F09.

What closes the finding

Unsigned, modified, expired and wrong-key events must be rejected before a ledger write. A correctly authenticated event must succeed once. Record rejection reason and correlation ID without storing authentication secrets.

signature: absent; simulator state: pending → settled; valid follow-up: blocked

PAYMENTS ENGINEERING LEAD / 23 SEP

Evidence EV-F02 · CWE-345 · ISO Annex A context 8.5 / 8.26 / 8.29

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Build identity crosses into production

CRITICAL / VERIFIED FIXED

CVSS 9.9

Build identity / production role

Business impact

A compromised low-privilege build workload could assume a role in a separate production authority. In the fixture, that role could read protected records, change a deployment and disable a seeded service.

Observed behavior

A valid token issued to an unprotected test branch satisfied an overly broad production trust policy. The assumed role permitted the three seeded actions above. The test stopped at disposable resources and did not establish organization-wide administrative access.

Why it happens

The role trust condition matched the repository but omitted the protected environment and intended branch. Its permissions also exceeded the deployment task's minimum requirements.

Limits of the evidence

The changed-scope CVSS assumption is explicit: the build system and production account enforce different security authorities. No long-lived credential theft or real service interruption is represented.

Required correction

Pin the workload identity subject, audience and protected environment. Require an approved deployment workflow, reduce the production role's actions and resources, and prevent unreviewed branches from requesting production identity.

What closes the finding

The original branch must fail to assume the role. The approved release path must still deploy only its intended service. Compare effective permissions and verify the denial is logged. The 21 September fixture satisfies these checks.

before: role assumption allowed; after: denied; protected release control: passed

HEAD OF PLATFORM ENGINEERING / CLOSED 21 SEP

Evidence EV-F03 + RT-F03 · CWE-269 · ISO Annex A context 8.2 / 8.3 / 8.9

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Invoice access trusts the supplied tenant

HIGH / OPEN

CVSS 8.1

`api.astervale.example / invoices`

Business impact

An ordinary merchant user could read or alter another tenant's invoice. This creates confidentiality and accounting-integrity exposure without requiring administrator access.

Observed behavior

A North merchant session requested the seeded South invoice while supplying South's tenant field. Both retrieval and a description update succeeded. The same session was denied by an adjacent endpoint that derived tenant membership from the session.

Why it happens

Authorization was implemented independently across handlers. The invoice handler relied on a request field while the adjacent handler used trusted session context, producing inconsistent object-level enforcement.

Limits of the evidence

One cross-tenant invoice and one harmless editable field were exercised. Bulk extraction, deletion, settlement and changes to real accounting data were excluded.

Required correction

Centralize object authorization and derive tenant context from authenticated membership. Apply it to reads, updates, exports and background jobs. Build a tenant-pair regression suite with ordinary and elevated roles.

What closes the finding

Run the role-by-tenant matrix across every invoice operation. Wrong-tenant requests must fail before mutation; valid same-tenant actions must succeed. Verify the audit record identifies the actor and rejected object reference.

North merchant → South invoice: read allowed; seeded description update allowed

API ENGINEERING LEAD / 06 OCT

Evidence EV-F04 · CWE-639 · ISO Annex A context 8.3 / 8.28 / 8.29

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Revoked operators retain active sessions

HIGH / OPEN

CVSS 8.1

Operator console / session service

Business impact

Removing an operator's role does not immediately remove their access. A departed or compromised operator could continue reading and changing privileged records until an existing session expires.

Observed behavior

The seeded operator's role was revoked at 11:00 UTC. Its already-issued session still read an administrative record and changed a harmless policy label at 11:20. A new login correctly received no operator role.

Why it happens

Authorization claims were cached for the full session lifetime. Resource handlers did not check a current privilege version or invalidate outstanding sessions after a role change.

Limits of the evidence

The demonstration covers a twenty-minute interval and two administrative actions. It does not establish the maximum surviving session lifetime or access through separate identity providers.

Required correction

Invalidate privileged sessions when roles or account status change. Enforce short-lived authorization state or a server-side privilege-version check. Provide emergency revocation covering all device sessions and service refresh tokens.

What closes the finding

After revocation, retry each active session and refresh path within the agreed revocation objective. All privileged actions must fail. Verify a new permitted operator session still works and the revocation is visible to responders.

role removed 11:00; old session privileged write 11:20: allowed; new login: denied

IDENTITY ENGINEERING LEAD / 06 OCT

Evidence EV-F05 · CWE-613 · ISO Annex A context 5.18 / 8.5 / 8.16

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Backup object is readable without identity

HIGH / VERIFIED FIXED

CVSS 7.5

Object storage / recovery snapshot

Business impact

Public read access to a recovery snapshot could disclose the data it contains. Encryption at rest does not prevent disclosure when the object service authorizes an anonymous download.

Observed behavior

An unauthenticated request retrieved a seeded backup marker through the object endpoint. The policy simulator also allowed anonymous reads for that object prefix. Listing and write operations were denied.

Why it happens

A temporary sharing policy remained attached to the recovery prefix after a migration exercise. The storage account's public-access guard was not enabled for that location.

Limits of the evidence

The fixture contains synthetic rows only. The result proves object readability, not the contents, retention period or historic access pattern of any real backup estate.

Required correction

Remove the public policy, enforce the platform's public-access guard and review equivalent prefixes through configuration inventory. Separate restore identities from application identities and review object-access telemetry for the exposure interval.

What closes the finding

Anonymous reads must fail at both the normal and direct object endpoints. An authorized restore identity must still restore the seeded object. The 21 September fixture demonstrates both outcomes.

anonymous GET before: 200; after: denied; authorized recovery control: passed

CLOUD OPERATIONS LEAD / CLOSED 21 SEP

Evidence EV-F06 + RT-F06 · CWE-732 · ISO Annex A context 8.3 / 8.9 / 8.13

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Connector can read an internal endpoint

MEDIUM / OPEN

CVSS 6.5

Partner connector / fetch worker

Business impact

A merchant who can configure a connector could make the server retrieve internal data that the merchant cannot reach directly. The application returns the fetched response to the caller.

Observed behavior

A connector configured for an approved test URL followed a redirect to a controlled internal service and returned its confidential fixture marker. The initial host check passed; the redirected destination was not revalidated.

Why it happens

Destination policy applied only to the submitted URL. Redirects and resolved addresses were trusted after the first validation step, while the worker retained broad network reachability.

Limits of the evidence

The internal endpoint was a benign test service. Cloud metadata, privileged credentials and third-party hosts were excluded; none is claimed to have been accessed.

Required correction

Restrict connector destinations by business requirement, validate each redirect and resolved address, and enforce egress policy outside the model and application process. Remove unneeded routes from the fetch worker.

What closes the finding

Test direct internal addresses, redirect chains, changed DNS responses and equivalent address encodings using approved fixtures. Disallowed destinations must fail while an approved partner fetch still succeeds.

approved URL → redirect → internal fixture; response marker returned to merchant

INTEGRATIONS ENGINEERING LEAD / 20 OCT

Evidence EV-F07 · CWE-918 · ISO Annex A context 8.20 / 8.22 / 8.26

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Shared cache serves a private report

MEDIUM / VERIFIED FIXED

CVSS 5.3

Portal edge / report response cache

Business impact

A limited private report response could be served from a shared cache to a later visitor. The fixture exposed a report title and summary marker, not a complete dataset.

Observed behavior

A signed-in user requested a seeded private report. A subsequent unauthenticated request to the same fixture URL received the cached title and summary. The response lacked an effective private or no-store directive at the edge.

Why it happens

A broad cache rule overrode the origin's intended authenticated-content handling. Cache keys did not isolate the response by the authorization context.

Limits of the evidence

The low confidentiality impact in CVSS reflects the deliberately limited response demonstrated. The test does not prove that every route, cache location or past response was affected.

Required correction

Bypass shared caching for authenticated reports and explicitly mark sensitive responses no-store. Purge affected cached objects, review rule precedence and test the effective edge behavior, not only origin headers.

What closes the finding

Warm the cache as one user, then request as an unauthenticated visitor and a different tenant. Neither may receive the private marker. Verify authorized delivery still works. The retest fixture passes at both test edge locations.

before: private marker served from shared cache; after: unauthenticated request denied

WEB PLATFORM LEAD / CLOSED 21 SEP

Evidence EV-F08 + RT-F08 · CWE-524 · ISO Annex A context 8.3 / 8.9 / 8.28

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Repeated payout requests apply twice

MEDIUM / OPEN

CVSS 6.5

Payout API / idempotency store

Business impact

An authenticated merchant could repeat a payout instruction and create a second ledger effect. Accidental retries could produce the same defect, making reliability and abuse prevention share one control.

Observed behavior

Two identical requests using the same idempotency key were submitted to the isolated ledger. Both returned success and created separate seeded state transitions after the first worker's cache entry expired.

Why it happens

Idempotency was enforced by a short-lived cache rather than an atomic constraint at the durable business-operation boundary. Its lifetime did not cover supported retry behavior.

Limits of the evidence

No live funds moved. Concurrency beyond the two controlled requests and other transaction types were not evaluated, so their behavior remains unknown.

Required correction

Enforce an atomic uniqueness rule scoped to the merchant and business operation. Bind the key to a canonical payload, retain it for the required retry interval and return the original result for legitimate repeats.

What closes the finding

Sequential and concurrent repeats must produce one durable effect. A reused key with a changed payload must fail clearly. Test retries across worker restarts and the full supported retry interval.

same merchant + key + body; accepted effects: 2; expected durable effects: 1

PAYMENTS ENGINEERING LEAD / 20 OCT

Evidence EV-F09 · CWE-841 · ISO Annex A context 8.26 / 8.28 / 8.29

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

Privilege changes lack a complete audit record

MEDIUM / OPEN

QUALITATIVE RATING

Operator console / audit pipeline

Business impact

Responders cannot reliably attribute a sensitive role change or reconstruct its before-and-after state. That gap can delay containment and weaken the evidence provided to management or an auditor.

Observed behavior

The fixture contains an application request for a role change and an identity-provider state update, but no joined administrative event with actor, affected user, old role, new role and decision. Ordinary sign-ins were recorded correctly.

Why it happens

The audit event was emitted by selected interface handlers instead of a common authorization and mutation boundary. One administrative path bypassed it, and cross-service correlation was incomplete.

Limits of the evidence

This is a control-effectiveness observation. It is assigned medium business priority without a CVSS score because the demonstrated issue is an evidence gap, not a directly scored exploit chain.

Required correction

Emit structured events for all privileged mutations and their denials from a common enforcement boundary. Include actor, subject, permission decision, before-and-after references, UTC time and correlation ID. Restrict audit writes and log audit exports and administrative access.

What closes the finding

Exercise each role-change path, failed request and automated administration route. Reconstruct every change from the audit store alone, including the responsible identity. Prove an ordinary administrator cannot rewrite prior events.

role mutation present; attributable joined audit event: missing; ordinary login event: present

SECURITY OPERATIONS LEAD / 20 OCT

Evidence EV-F10 · CWE-778 · ISO Annex A context 8.15 / 8.16 / 5.28

No exploit score assigned. Priority is based on the demonstrated audit-evidence gap.

Legacy listener permits a weak TLS suite

LOW / VERIFIED FIXED

CVSS 3.7

Legacy partner listener

Business impact

The legacy listener permits a cryptographic configuration that may weaken confidentiality under demanding attack conditions. The assessment did not recover plaintext or establish a practical interception opportunity.

Observed behavior

A controlled handshake successfully negotiated a deprecated cipher suite on the legacy listener. The primary public gateway rejected the same proposal, limiting the observed issue to one configuration path.

Why it happens

The legacy listener retained a manually maintained TLS profile outside the standard gateway configuration baseline and its change-review checks.

Limits of the evidence

The CVSS vector assumes high attack complexity and limited confidentiality impact. Cipher acceptance is the demonstrated condition; decryption and active interception were not attempted.

Required correction

Move the listener to the approved TLS baseline, remove deprecated suites and inventory exceptional listeners. Validate partner compatibility before rollout and include effective listener configuration in recurring checks.

What closes the finding

The deprecated proposal must fail on the original listener and its failover endpoint. Approved protocol and cipher combinations must still complete a handshake. Both checks pass in the retest fixture.

deprecated suite before: accepted; after: rejected; approved handshake: passed

INFRASTRUCTURE OPERATIONS LEAD / CLOSED 21 SEP

Evidence EV-F11 + RT-F11 · CWE-327 · ISO Annex A context 8.9 / 8.20 / 8.24

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Diagnostics disclose internal implementation details

LOW / OPEN

CVSS 3.1

Authenticated support diagnostics

Business impact

An authenticated user can obtain internal service names and a build path from an uncommon error condition. This information can assist further investigation, but no secret, credential or direct privileged action was demonstrated.

Observed behavior

A specific invalid state in the seeded support workflow returned an internal exception record. The response included a worker hostname and source location; ordinary validation failures returned a safe error identifier.

Why it happens

The exceptional error handler serialized the underlying exception object instead of the approved public error shape. The rare workflow state was absent from regression coverage.

Limits of the evidence

High attack complexity reflects the prerequisite workflow condition. Only implementation metadata was exposed. The fixture contains no user secrets, personal records or exploitable payload.

Required correction

Return a stable public error identifier and keep implementation details in restricted server logs. Apply the same response contract to asynchronous failures and verify that logging itself excludes credentials and sensitive payloads.

What closes the finding

Recreate the original workflow state and inspect the response as an ordinary user. Internal hostnames, stack traces and paths must be absent, while the correlation ID must allow an authorized responder to find the internal error.

rare workflow error → internal worker name and source path; no secret material

CUSTOMER PLATFORM LEAD / 20 OCT

Evidence EV-F12 · CWE-209 · ISO Annex A context 8.12 / 8.28 / 8.29

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

Fix the cause. Keep the proof.

24 HOURS

Contain the two critical entry points

F01 and F02: remove unauthenticated report operations and unverified payout state changes. Preserve affected configuration and event history for review.

Gate: original unauthorized paths fail.

14 DAYS

Unify identity and tenant enforcement

F04 and F05: centralize object access checks and propagate operator revocation to active sessions. Test role-by-tenant and session-lifecycle matrices.

Gate: negative cases fail; legitimate actions pass.

30 DAYS

Close the remaining open work

F07, F09, F10 and F12: constrain connector egress, enforce durable idempotency, complete administrative audit records and normalize diagnostics.

Gate: each finding meets its written acceptance test.

90 DAYS

Make regression visible

Extend coverage to deferred recovery and identity scenarios. Add the corrected failure modes to release checks and agree a recurring validation schedule.

Gate: known paths stay closed across new releases.

Closed is an evidence state.

A change ticket or a developer assertion is not a retest result. These four fixture records include the original failure, the updated boundary and a legitimate control that still succeeds.

Finding	Negative case	Positive control
F03 / Build role	Unprotected branch cannot assume production role.	Protected release deploys only the intended service.
F06 / Backup	Anonymous reads denied at normal and direct endpoints.	Authorized restore identity retrieves seeded backup.
F08 / Cache	Anonymous and wrong-tenant requests receive no private marker.	Intended user can retrieve their report.
F11 / TLS	Deprecated suite rejected on listener and failover.	Approved handshake completes successfully.

Eight findings remain open

F01, F02, F04, F05, F07, F09, F10 and F12 have no passing retest in this edition. A planned fix is not represented as a partial closure.

Regression is a new event

If the same failure reappears after a release, reopen the record with a new observation and affected version. Preserve the earlier successful retest rather than rewriting history.

Useful to an auditor. Honest about its limits.

Selected ISO/IEC 27001:2022 Annex A references help an assurance team locate relevant technical evidence. Applicability and the wider control conclusion belong to the organization's ISMS and audit process.

Control context ¹	Evidence in this sample	Additional evidence needed
8.2 / 8.3 · Privileged and object access	F01, F03, F04; RT-F03	Access policy, approvals, periodic review and wider population.
8.5 · Authentication	F02, F05; privileged sign-in scenario	Identity lifecycle, recovery paths and implementation coverage.
8.8 / 8.9 · Vulnerabilities and configuration	Register, owners and four retests	Asset completeness, remediation process and exception history.
8.15 / 8.16 · Logging and monitoring	F10; detection exercise matrix	Retention, alert ownership, access control and operating evidence.
8.26 / 8.29 · Application requirements and testing	F01, F02, F04, F09	Secure development requirements and repeated release evidence.

¹ Context labels are shortened editorial descriptions. No ISO certification, control pass rate, Statement of Applicability or conformity opinion is issued by this report.

One evidence base. Several useful lenses.

Lens	Use in this report	Do not infer
NIST CSF 2.0 / Govern	Decision owners, scope approval and time-bound exceptions.	Enterprise governance effectiveness from a technical test.
Identify / Protect	Asset scope, trust boundaries and access-control findings.	Complete asset inventory or full preventive coverage.
Detect / Respond	Observed event, alert and triage outcomes; F10 evidence gap.	Detection of every attacker or a tested full incident plan.
Recover	Authorized restore read used as a positive control in F06.	Successful disaster recovery; the full drill was deferred.
OWASP WSTG	Web test design for identity, authorization, configuration and business logic.	Completion of every WSTG case or a certification.
MITRE ATT&CK T1078	Context for account and privilege misuse in F03 and F05.	Coverage of every technique or attribution to an actor.

PRACTICAL USE

Attach the finding, the scope and its retest evidence together. A control label without those records is a categorization, not assurance.

An accountable agent.

An accountable platform.

The intended audit trail covers customers and staff as well as models, tools and services. A timeline of model activity alone cannot explain who authorized, changed, viewed or exported the work.

Actor class	Events to retain
Customer / administrator	Sign-in, role changes, domain verification, scope changes, cadence and budget changes, report views, download requests and export delivery.
Model / worker	Model and harness version, proposed action, policy decision, target, tool invocation, result, failure, stop and human override.
Reviewer / service	Finding edits, severity changes, approvals, retest decisions, report versions, integration sync results and audit-store administration.

Minimum event envelope

UTC timestamp, actor and tenant, action, resource, permission decision, correlation ID, scope revision and evidence reference. Redact credentials and keep sensitive content behind access controls.

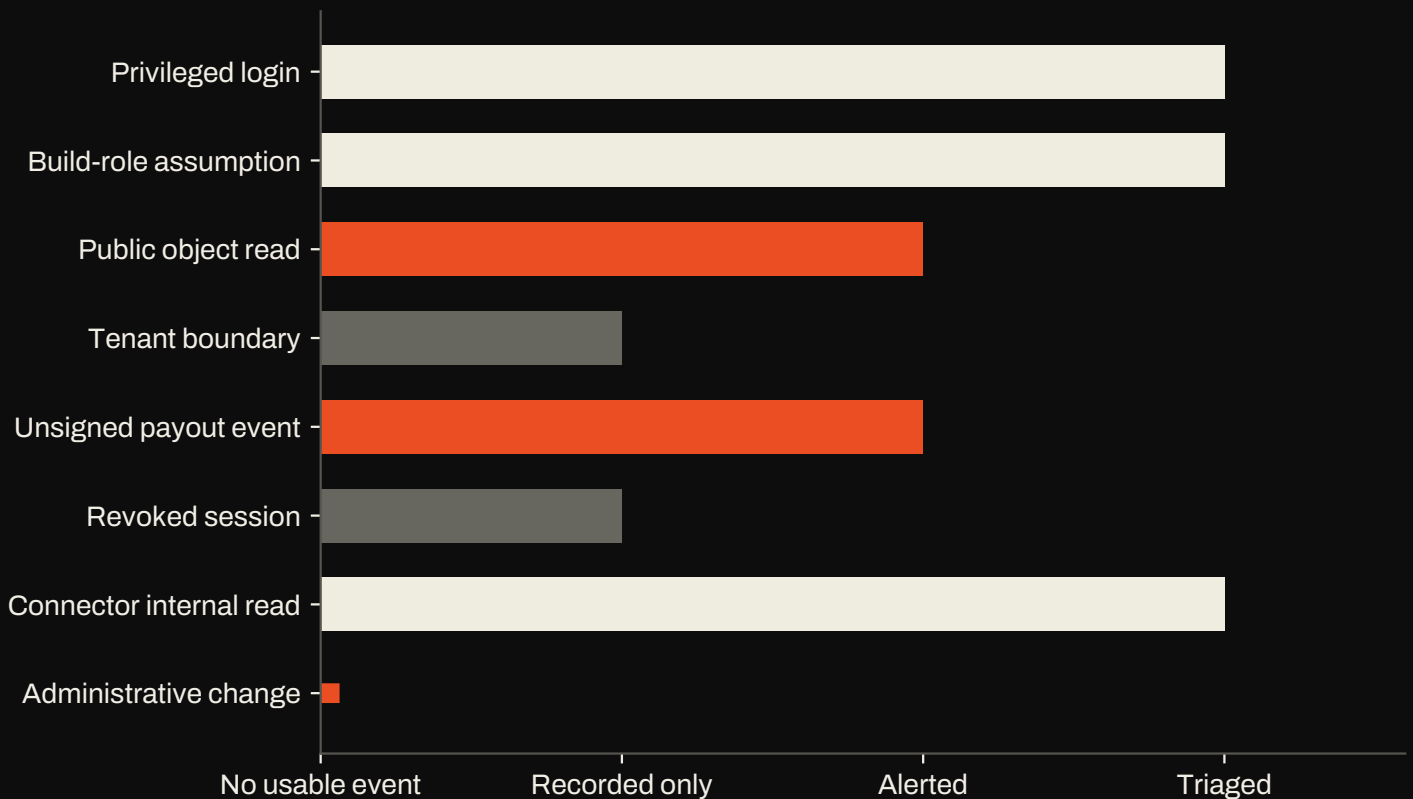
Integrity requires operations

Use restricted append paths, durable storage, retention policy and independent integrity checkpoints. Hash linking detects some alterations; it does not prevent an administrator replacing an entire unanchored chain.

THE INCLUDED JSONL IS A SYNTHETIC EVENT-SCHEMA EXAMPLE, NOT A LIVE AUDIT EXPORT.

An event is not an investigation.

Eight selected fixture scenarios illustrate the distance between telemetry and response. These scenarios are a subset of the 28 completed detection-and-response check cases.



Three reached analyst triage; two generated an alert without a completed triage record; two were recorded only; one produced no usable joined event. The categories are mutually exclusive end states.

Next exercise: repair F10 attribution, assign an owner to each alert and measure time from event to a documented response decision. This sample supplies no invented response-time benchmark.

Fresh reports. Visible evidence age.

A daily report can be rebuilt from the latest available evidence. It must show when each system was last tested. A new publication timestamp does not make an old observation current.

Customer choice	What changes	What stays visible
Focused baseline	A scheduled, agreed scope with a reserved retest allowance.	Untested assets and the age of each observation.
More frequent validation	More run windows or wider coverage within an agreed budget.	Actual completed checks, remaining budget and deferred work.
Change-triggered checks	Prioritize new releases or material configuration changes.	Trigger, approved scope, cost estimate and execution decision.
Daily assurance edition	Refresh findings, owners, closure state and explanatory reporting.	Last test time separately from report generation time.

A visible customer control

Before a cadence change is accepted, show estimated spend, included assets, depth and the retest reserve. Log the approving user and retain the previous schedule.

A sensible work queue

Prioritize material changes and open high-impact paths. Do not use an idle GPU budget as permission to widen scope or make an intrusive test more frequent.

The things we cannot conclude.

01 No exhaustive assurance

A finite assessment cannot prove the absence of vulnerabilities. Outcomes apply to the stated estate, versions, identities, windows and checks.

02 No financial-loss estimate

Transaction-integrity scenarios illustrate technical effects in a simulator. They do not quantify fraud likelihood, expected loss or insurance coverage.

03 No real customer exposure

All records in this report were authored as fixtures. There was no customer scan, exploit, remediation deployment or independent human-assessor sign-off.

04 No universal compliance verdict

Technical evidence can support an audit. It cannot replace the wider management-system, operational and documentary evidence required for a conformity decision.

05 No automatic supplier coverage

The full recovery drill, secondary identity provider and unapproved third parties remain outside completed assurance. A customer must authorize and resource that additional work.

Proof has an address.

The companion ZIP contains 12 authored observation records, four authored retest records, a 12-event audit fixture and a SHA-256 manifest. These are reproducible sample files, not captured traffic.

Fixture file	SHA-256 prefix · full hash in manifest
EV-F01.json	23778e32cde0fdaf1ffd44ae
EV-F02.json	b599af0a3e23dbd2f7282ab9
EV-F03.json	1ae58f85e42b94e58a0ac68a
RT-F03.json	bb7b141b1eb0426b0b05df2b
EV-F04.json	11148b010a4a4992001181db
EV-F05.json	85a4ca6cef0160bf70aa335e
EV-F06.json	10dcda7689d4fe2f133ff555
RT-F06.json	ed74c63034a0e70a6f9e1254
EV-F07.json	bfa759d90e3cde99983f8c7b
EV-F08.json	3cef0d165b97e4b46b3bab34
RT-F08.json	87ba20f75afa805007ae9742
EV-F09.json	07118ec9f29100c9272e700b
EV-F10.json	04acf148902e0aab7b60a96c
EV-F11.json	67a83e860c4f06e8d8f7d295
RT-F11.json	21a3657322550aa503bb0626
EV-F12.json	37e177036eeaceff90290382
audit-fixture.jsonl	1f4c8e5e0084afbeeb98d4989

Hashes let a recipient check that downloaded fixture files match the manifest. They do not establish the truth of an observation or an independent chain of custody. The PDF hash is published separately to avoid self-reference.

Built on established assessment practice.

- 01** **extbfNIST SP 800-115** [↗](#)
Planning, execution and reporting of technical assessments.
- 02** **extbfFIRST CVSS v3.1** [↗](#)
Technical base-score definitions; vectors shown with each scored finding.
- 03** **extbfISO/IEC 27001:2022** [↗](#)
ISMS context; selected Annex A references are editorial mappings.
- 04** **extbfNIST Cybersecurity Framework** [↗](#)
Govern, Identify, Protect, Detect, Respond and Recover lenses.
- 05** **extbfOWASP Web Security Testing Guide** [↗](#)
Web assessment methodology and test-family inspiration.
- 06** **extbfMITRE ATT&CK / T1078** [↗](#)
Account-misuse context for the illustrated identity scenarios.
- 07** **extbfCure53 / Forward Email, September 2026** [↗](#)
Public example of scoped work packages and detailed finding records.
- 08** **extbfNCC Group / Google Confidential Space, July 2025** [↗](#)
Public example of threat-model context, limitations and structured findings.

Sources reviewed 22 September 2026. No vendor findings, proprietary report text or certification marks are reproduced. Case content and design are original adaptations.

SEE THE RISK. UNDERSTAND IT. CLOSE IT.

INTELLIGENCE, MADE ACCOUNTABLE.

For the operator who needs the evidence.
For the executive who needs the decision.
For the auditor who needs the trail.

[decima.systems/reports/sample/](#) ↗

Public sample / A proposed Decima reporting standard / No live assessment