API Security Assessment

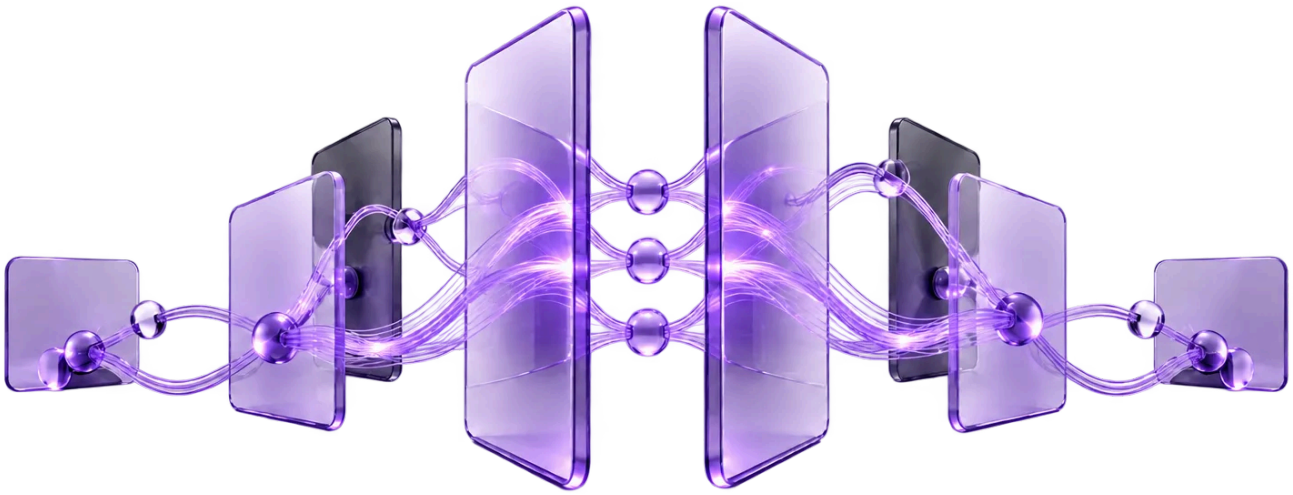
Avelune Logistics

01 September 2026 - 05 September 2026

Prepared by Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL



1. Document control

Version	Issued	Author	Review
1.0.0	2026-09-17	Julien Perrin	Sophie Roux / 16 September 2026

Authorized distribution

Restricted distribution. Intended roles: Camille Moreau, API lead; Julien Perrin, assessment author; Sophie Roux, quality reviewer.

This report describes observations within the agreed scope and assessment period. Subsequent changes may affect its conclusions. Distribution is restricted to authorized recipients.

Revision history

Version 1.0.0 issued 2026-09-16. Initial assessment period 1-5 September 2026; editorial review completed 16 September 2026. No remediation retest has yet taken place.

Table of Contents

2. Executive assessment

Assessment conclusion	Action required
3 findings affect Partner API v2.8: 1 High, 1 Medium, 1 Low. The assessment reviewed the agreed configuration and application records against the approved service baseline. Correction priorities reflect the impact, required access and dependencies documented in each finding.	Assign F-1 to Camille Moreau, API lead for correction by 30 September 2026. Address F-2 and F-3 by 16 October 2026, then perform the documented acceptance checks before closure.

Verified controls

The sampled endpoints reject unauthenticated requests, and account identifiers are used throughout the assessment.

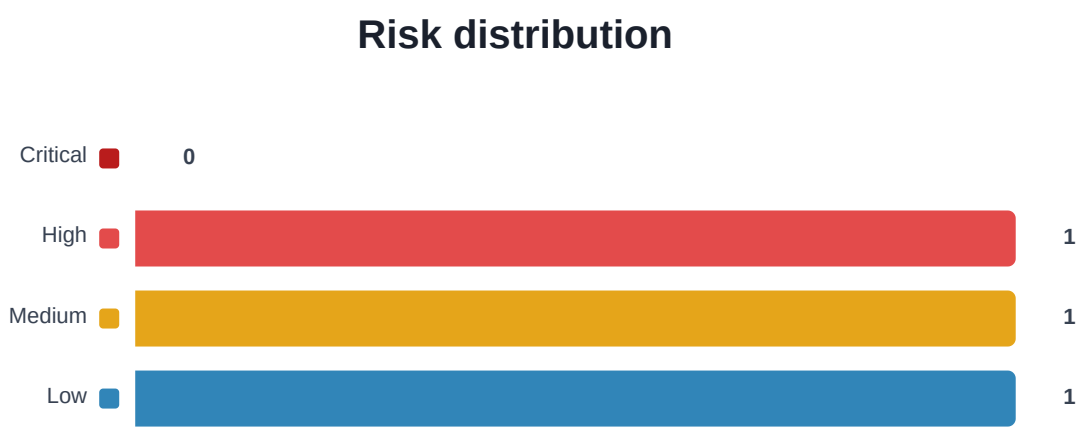
3. Assessment analysis

The assessment of Partner API v2.8 identified 3 findings: 0 Critical, 1 High, 1 Medium, 1 Low. Twenty-four documented endpoints, three application roles and two partner accounts. Documentary review and non-destructive checks in staging; production and external payment processing excluded.

The principal improvement concerns sensitive responses lack an explicit cache policy. A client or intermediary may retain personal data longer than intended. No retrieval by an unauthorized person is asserted. Correction ownership rests with Camille Moreau, API lead. The priority is to reduce this exposure without interrupting the service's required business functions.

The remaining observations concern application errors disclose internal implementation details and revoked sessions remain accepted beyond the required interval. They require separate acceptance criteria because changing one policy does not establish that the other controls operate effectively. Review effective runtime behavior as well as the saved configuration.

The sampled endpoints reject unauthenticated requests, and account identifiers are used throughout the assessment. These controls provide a basis for remediation, but their presence does not compensate for the documented exceptions. The action plan separates implementation evidence from successful retest results.



4. Scope and conditions

The following register defines the assessed assets, access conditions and accountable owners.

API / version	Environment	Roles / tenants	Business owner
Partner API v2.8	Staging / partner-api.avelune.example	Partner reader, operator and administrator; two tenants	Camille Moreau, API lead

Detailed scope register

Twenty-four documented endpoints, three application roles and two partner accounts. Documentary review and non-destructive checks in staging; production and external payment processing excluded.

Exclusions and restrictions

Only the supplied staging assets and evidence are in scope. Production changes, disruption, social engineering and third-party systems are excluded. Sampling does not establish complete coverage.

5. Assessment coverage

Record the method, reference version, observation date and supporting evidence for each assessed area. A reference mapping does not constitute certification.

Assessment area	Status	Evidence / reference
Endpoint inventory and coverage	Verified	E-00: 24-endpoint inventory
Authentication and session lifecycle	Gap observed	E-03: revocation timeline
Object and function authorization	Not tested	Excluded: full authorization matrix
Tenant isolation	Not tested	Excluded: tenant-isolation testing
Input handling and resource limits	Gap observed	E-02: error handling review
Business workflow integrity	Not tested	Excluded: business workflow testing

Allowed statuses: Verified, Gap observed, Not tested, Not applicable. Justify exclusions and not-applicable decisions.

Coverage rationale

Configuration and documentary evidence were reviewed from 1 to 5 September 2026. Each observation is linked to E-01, E-02 or E-03. Areas without evidence remain Not tested; a successful sampled check does not imply coverage of the entire environment.

Reference: engagement baseline DEMO-2026-09, revision 1.0, approved for this engagement.

6. Environment context

Assessed environment

Partner API v2.8. Staging / partner-api.avelune.example. Service ownership: Camille Moreau, API lead. The evidence bundle is frozen at assessment close; later changes are outside this issue.

Evidence requirements

Record the endpoint, HTTP method, tested role and tenant, expected authorization, observed response and timestamp. Attach redacted evidence without live credentials.

Evidence register

E-01: E-01: redacted response-header review, 3 September 2026, build 2.8.14. Six of six profile responses lacked Cache-Control.

E-02: E-02: three validation-error records from the staging support bundle, dated 4 September 2026.

E-03: E-03: revocation timeline, 5 September 2026; initial revocation 10:00 UTC, validation still active at 10:12 UTC.

7. Findings register

Findings use the report order. Keep the same reference in the action plan and retest record.

F-1 Sensitive responses lack an explicit cache policy

FINDING F-1	Low / 3.3 / 10

F-2 Application errors disclose internal implementation details

FINDING F-2	Medium / 4.3 / 10

F-3 Revoked sessions remain accepted beyond the required interval

FINDING F-3	High / 7.1 / 10

8. Sensitive responses lack an explicit cache policy

FINDING F-1	Low / 3.3 / 10

Observation and affected context

The six sampled customer-profile responses did not declare a cache policy. The approved API baseline requires no-store for personal account data.

Technical analysis

The missing directive concerns the HTTP response, independently of transport encryption and endpoint authentication. A successful authorization decision does not express whether a representation may be retained. The application and gateway must agree on the effective policy; a header configured in source code is insufficient if an intermediary removes or replaces it.

Affected scope and limits

The observation covers six profile responses in the supplied staging bundle, not every route. It establishes a policy omission, not a demonstrated shared-cache disclosure. Browser history, service-worker storage and application-managed offline data require separate lifecycle controls.

Impact

A client or intermediary may retain personal data longer than intended. No retrieval by an unauthorized person is asserted.

- Confidentiality: retained profile data may outlive the session on a shared client or in an operational diagnostic capture.
- Business consequence: the service owner cannot demonstrate the intended retention boundary for personal account responses. No cross-tenant access, integrity loss or service outage was demonstrated.

Correction

Apply the approved cache policy centrally, cover success and error responses, and retain a regression test for sensitive endpoints.

1. Set Cache-Control: no-store for classified sensitive responses at the application or gateway policy layer. Do not substitute no-cache, which permits storage subject to revalidation.
2. Inventory profile, account-export and sensitive error responses; document deliberate exceptions for genuinely public content. Ensure downstream header transformations preserve the policy.
3. Add contract tests to the release pipeline and review client-side offline storage separately. Assign ownership of both the application configuration and the gateway override.

Accountable owner: Camille Moreau, API lead. Preserve release and rollback evidence before requesting closure.

9. Supporting evidence

F-1 / Sensitive responses lack an explicit cache policy

evidence record

E-01: redacted response-header review, 3 September 2026, build 2.8.14. Six of six profile responses lacked Cache-Control.

E-01 / API SECURITY

Reviewed item	Scope	Recorded state
Sample	6 of 6 profile responses	Cache-Control absent
Required state	Sensitive response policy	Cache-Control: no-store

Evidence register / Review window: 01-05 September 2026

E-01 - Reviewed record extract, September 2026.

Acceptance criterion

Repeat the six response checks and verify the approved policy on every result.

Closure evidence to collect

1. Record the effective response headers for the same six records, including the serving build and gateway route.
2. Verify success and relevant error responses against the approved policy; retain sanitized results without profile bodies.
3. Confirm ordinary profile rendering and sign-out behavior remain functional. A header check alone does not prove that previously stored copies have been removed.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS v3.1: 3.3 (Low)
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Response policy

```
Cache-Control: no-store
Content-Type: application/json
Vary: Authorization
```

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-01.

OWASP REST Security Cheat Sheet

10. Application errors disclose internal implementation details

FINDING F-2	Medium / 4.3 / 10

Observation and affected context

Three redacted error records contain internal module names and an application stack trace. The public error contract requires a generic message and correlation identifier.

Technical analysis

The response boundary exposes diagnostic detail intended for operators: internal module identifiers and stack frames. Client-facing error serialization should be distinct from server-side exception logging. Validation failures and unexpected exceptions may use different handlers, so normal-path testing alone does not establish consistent sanitization.

Affected scope and limits

The three records support an information-disclosure finding only. They do not establish access to source code, secret material or a vulnerable dependency version. The review did not exercise exception-triggering payloads against a live service.

Impact

Internal implementation details increase unnecessary information exposure and complicate support-data handling. No credentials appeared in the sample.

- Confidentiality: internal naming and implementation structure become available beyond the support team that needs them.
- Operational impact: inconsistent error contracts complicate client handling and encourage excessive diagnostic collection. The local exposure reflects limited exposed detail and the absence of secrets in the reviewed sample.

Correction

Return generic client-facing errors and keep detailed traces in access-controlled server logs.

1. Centralize exception-to-response mapping with stable public error codes, appropriate HTTP status and an opaque correlation identifier.
2. Keep stack traces in restricted server logs; apply redaction before persistence and avoid including request credentials or full sensitive bodies.
3. Cover validation, authorization and unexpected-error handlers in automated response-schema tests. Review gateway-generated errors as a separate path.

Accountable owner: Camille Moreau, API lead. Preserve release and rollback evidence before requesting closure.

11. Supporting evidence

F-2 / Application errors disclose internal implementation details

evidence record

E-02: three validation-error records from the staging support bundle, dated 4 September 2026.

E-02 / API SECURITY

Reviewed item	Scope	Recorded state
Sample	3 redacted error records	Internal module names / stack trace
Expected boundary	Public response vs. operator log	Generic response; restricted diagnostics

Evidence register / Review window: 01-05 September 2026

E-02 - Reviewed record extract, September 2026.

Acceptance criterion

Confirm generic errors in the reviewed cases and verify that correlation identifiers still support diagnosis.

Closure evidence to collect

1. For the three recorded cases, compare corrected response schemas with the public API contract; no stack frame, filesystem path or internal module identifier should remain.
2. Use each correlation identifier to locate the corresponding restricted diagnostic event without adding sensitive details to the response.
3. Confirm the API still distinguishes client errors from server failures and preserves support triage information.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS v3.1: 4.3 (Medium)

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

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Public error contract

```
{
  "error": "validation_failed",
  "correlationId": "req-20260904-021"
}
```

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-02.

OWASP REST Security Cheat Sheet - error handling

12. Revoked sessions remain accepted beyond the required interval

FINDING F-3	High / 7.1 / 10

Observation and affected context

The supplied session-validation record shows a revoked session still marked active after twelve minutes. The agreed partner-access requirement is five minutes.

Technical analysis

Administrative revocation changes the authoritative session state, but serving instances may continue to rely on cached validation decisions. Token expiry, refresh-token invalidation and immediate access-session revocation are separate controls. The evidence establishes a timing mismatch; it does not identify whether cache TTL, propagation delay or a missing validation path caused it.

Affected scope and limits

The timeline contains an active validation result twelve minutes after revocation, against a five-minute contractual bound. It does not establish an indefinite bypass or compromise of signing keys. Other instances and session types were not covered by this record.

Impact

A session removed by an administrator can retain access beyond the agreed revocation window.

- Access control: a previously authorized session may continue to act with its existing permissions after an administrator expects removal to take effect.
- Incident response: containment and employee or partner offboarding become less predictable. The possible scope is bounded by that session's permissions and remaining validity; privilege escalation is not demonstrated.

Correction

Align session validation and revocation propagation with the five-minute requirement; document the behavior of distributed caches.

1. Document the authoritative revocation state and every cache or validation layer that consumes it. Define a measurable maximum propagation interval.
2. Implement bounded cache validity or reliable invalidation so the five-minute requirement holds on every serving instance. Review behavior when the state store is unavailable.
3. Treat access and refresh credentials explicitly, record revocation timestamps in UTC and monitor propagation delays without logging credential values.

Accountable owner: Camille Moreau, API lead. Preserve release and rollback evidence before requesting closure.

13. Supporting evidence

F-3 / Revoked sessions remain accepted beyond the required interval

evidence record

E-03: revocation timeline, 5 September 2026; initial revocation 10:00 UTC, validation still active at 10:12 UTC.

E-03 / API SECURITY

Reviewed item	Scope	Recorded state
Revocation	10:00 UTC	Administrative state changed
Deadline	10:05 UTC	Session must be rejected
Recorded state	10:12 UTC	Still active; requirement exceeded

Evidence register / Review window: 01-05 September 2026

E-03 - Reviewed record extract, September 2026.

Acceptance criterion

A revoked session is rejected within five minutes across each serving instance.

Closure evidence to collect

1. Collect sanitized, timestamped session-state results from all serving instances using a dedicated staging identity.
2. Confirm rejection by the agreed deadline and continued validity of an unrelated control session.
3. Verify refresh behavior and recovery after a cache restart. Retain timestamps, instance identifiers and result codes, not bearer tokens.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS v3.1: 7.1 (High)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Session validation policy

```
revocationCache:
  maximumAgeSeconds: 300
  invalidateOnLogout: true
  failClosedOnValidationError: true
```

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-03.

OWASP Session Management Cheat Sheet

14. Remediation and retest

Finding	Owner / target	Status	Acceptance evidence
F-1 to F-3	Camille Moreau, API lead / 30 Sep-16 Oct 2026	Open; retest pending	Finding-specific acceptance checks in the action plan

Action plan

F-1: Camille Moreau, API lead. Target 30 September 2026. Repeat the six response checks and verify the approved policy on every result.

F-2: Camille Moreau, API lead. Target 16 October 2026. Confirm generic errors in the reviewed cases and verify that correlation identifiers still support diagnosis.

F-3: Camille Moreau, API lead. Target 16 October 2026. A revoked session is rejected within five minutes across each serving instance.

Retest record

Not retested as of 16 September 2026. Proposed retest window: 19-20 October 2026, subject to delivery evidence. All three findings remain Open; no correction or risk acceptance is asserted.

15. Rating and limitations

Rating method

Technical vulnerabilities use CVSS v3.1. Each scored finding includes its vector and prerequisites. Business priority also considers exposure and service dependencies. Control-assurance and governance observations are rated contextually and marked Not applicable for CVSS. CVSS is owned by FIRST and used by permission.

Residual uncertainty

Conclusions apply to the recorded configuration versions and assessment window. Untested areas are listed in the coverage register. Changes after evidence collection require revalidation. All findings remain open until the documented acceptance evidence has been reviewed.

Technical severity and remediation priority may differ. Document the reason when exposure, business context or correction dependencies change the order of work.