iOS Application Assessment

Sereine Mobilite

01 September 2026 - 05 September 2026

Prepared by Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL

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: Elise Laurent, mobile engineering 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

Executive assessment

3 findings affect Sereine Travel 4.6.2 (build 46218): 0 High, 1 Medium, 2 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.

Priority actions	Verified strengths
Assign F-1 to Elise Laurent, mobile engineering 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.	The reviewed session credential is stored in the platform credential store, and the application requests only the documented runtime permissions.

Assessment analysis

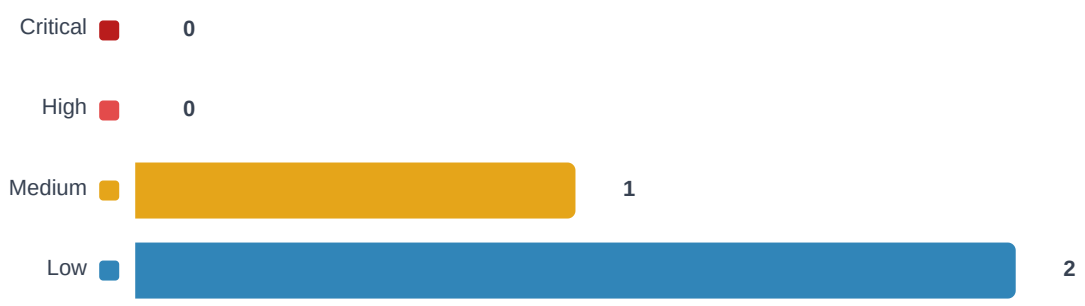
The assessment of Sereine Travel 4.6.2 (build 46218) identified 3 findings: 0 Critical, 0 High, 1 Medium, 2 Low. One staging build, two test devices and two user profiles. Local storage, session lifecycle, privacy and UI review; backend authorization, payment processing and modified-device testing excluded.

The principal improvement concerns personal trip details remain visible in the app switcher. A person viewing the unlocked device may see personal travel information outside the active application. Correction ownership rests with Elise Laurent, mobile engineering lead. The priority is to reduce this exposure without interrupting the service's required business functions.

The remaining observations concern diagnostic logs retain personal account details and cached trip documents remain after sign-out. 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 reviewed session credential is stored in the platform credential store, and the application requests only the documented runtime permissions. 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.

Risk distribution



Scope and conditions

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

App / build	Device / iOS	Test account	Distribution channel
Sereine Travel 4.6.2 (build 46218)	iPhone 14 and 15 / iOS 18.6	Two passenger profiles	Internal staging / TestFlight

Detailed scope register

One staging build, two test devices and two user profiles. Local storage, session lifecycle, privacy and UI review; backend authorization, payment processing and modified-device testing 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.

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
Local storage and Keychain	Gap observed	E-03: session-specific cache
Authentication and session lifecycle	Gap observed	E-03: sign-out data lifecycle
Network communication	Not tested	Backend and transport testing excluded
Platform permissions and app links	Verified	E-00: documented permission review
Privacy and sensitive UI content	Gap observed	E-01/E-02: personal data exposure
Build integrity and dependencies	Not tested	Build integrity not assessed

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.

Application and build profile

Assessed environment

Sereine Travel 4.6.2 (build 46218). com.sereine.example.travel / two supported test devices. Service ownership: Elise Laurent, mobile engineering lead. The evidence bundle is frozen at assessment close; later changes are outside this issue.

Evidence requirements

Record build, device, iOS version, user state and observation time. Number screenshots and redact personal data. Distinguish simulator results from device observations.

Evidence register

E-01: E-01: redacted app-switcher captures from both test devices, build 46218, 3 September 2026.

E-02: E-02: redacted diagnostic bundle containing twelve account events, 4 September 2026.

E-03: E-03: before-and-after cache inventory for a account, 5 September 2026; two documents persist after sign-out.

Findings register

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

F-1 Personal trip details remain visible in the app switcher

FINDING F-1	Low / 2.4 / 10

F-2 Diagnostic logs retain personal account details

FINDING F-2	Low / 3.3 / 10

F-3 Cached trip documents remain after sign-out

FINDING F-3	Medium / 4.6 / 10

Personal trip details remain visible in the app switcher

FINDING F-1	Low / 2.4 / 10

Observation and affected context

The supplied app-switcher captures show the passenger name and upcoming trip after the application moves to the background.

Technical analysis

The system app-switcher representation can retain the last rendered sensitive view when the application loses its active state. This representation has a different lifecycle from the live view controller; clearing an in-memory model later does not establish that the captured presentation is sanitized.

Affected scope and limits

Both supplied test-device captures show passenger and trip data. The observation concerns visual exposure to somebody able to view the device interface. It does not establish remote screenshot access, a sandbox escape or a bypass of device authentication.

Impact

A person viewing the unlocked device may see personal travel information outside the active application.

- Privacy: passenger identity and upcoming travel may be visible outside the active application screen.
- User expectation: navigating away from a sensitive view does not necessarily conceal its content. The local exposure reflects the local viewing prerequisite and the absence of remote access evidence.

Correction

Mask sensitive views when the application becomes inactive and restore them only when the appropriate user state is established.

1. Present an opaque privacy view when a sensitive scene becomes inactive, early enough to cover the system snapshot lifecycle.
2. Handle each supported scene and sensitive screen consistently, including modal presentations. Restore content only after the intended foreground and authentication state is re-established.
3. Ensure the privacy layer contains no personal labels or image previews and does not introduce an accessibility or navigation regression.

Accountable owner: Elise Laurent, mobile engineering lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-1 / Personal trip details remain visible in the app switcher

evidence record

E-01: redacted app-switcher captures from both test devices, build 46218, 3 September 2026.

E-01 / IOS APPLICATION

Reviewed item	Scope	Recorded state
Device coverage	2 supported test devices	Personal trip data visible
Expected state	Inactive sensitive scene	Opaque, non-personal presentation

Evidence register / Review window: 01-05 September 2026

E-01 - Reviewed record extract, September 2026.

Acceptance criterion

No personal trip details appear in app-switcher captures on either supported test device.

Closure evidence to collect

1. Review sanitized app-switcher captures from both supported devices and the same sensitive screens.
2. Include normal background transitions and supported interruption paths; record the OS version and application build.
3. Confirm returning to the application restores the correct user state without exposing the previous account during transitions.

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: 2.4 (Low)

CVSS:3.1/AV:P/AC:L/PR:N/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.

Privacy lifecycle

```
func sceneWillResignActive(_ scene: UIScene) {
    privacyCover.isHidden = false
}
// Remove the cover after foreground authentication is complete.
```

References

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

OWASP MASVS-STORAGE-2 - unintended data leakage

Diagnostic logs retain personal account details

FINDING F-2	Low / 3.3 / 10

Observation and affected context

The staging diagnostic bundle includes email addresses and booking references in normal application event records.

Technical analysis

Normal diagnostic events include account identifiers that are not required for the described support purpose. An application sandbox protects local files from ordinary peer applications, but support export deliberately moves those records to another processing boundary. Redaction must therefore occur before persistence or export, not only in the support user interface.

Affected scope and limits

Twelve account events contain email addresses or booking references. No real passenger data, access token or external disclosure was observed. The report does not establish the production logging level or retention configuration beyond the supplied staging bundle.

Impact

Diagnostic exports may disclose unnecessary personal information to support personnel or downstream log consumers.

- Confidentiality: support recipients and downstream log consumers may receive more personal data than needed to diagnose an issue.
- Data lifecycle: diagnostic copies can persist outside the application's sign-out cleanup. The impact depends on export access and retention; no regulatory breach or actual unauthorized recipient is asserted.

Correction

Minimize logged personal data, redact identifiers where appropriate and define retention and support-bundle access rules.

1. Define an allowlist of diagnostic fields and replace personal identifiers with scoped, non-sensitive correlation values where support needs linkage.
2. Apply structured redaction at the logging boundary and verify release-build behavior as well as staging. Exclude credentials, document contents and full personal payloads.
3. Set documented retention, access and deletion rules for support bundles. Ensure telemetry SDKs and crash reporting follow the same data-minimization policy.

Accountable owner: Elise Laurent, mobile engineering lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-2 / Diagnostic logs retain personal account details

evidence record

E-02: redacted diagnostic bundle containing twelve account events, 4 September 2026.

E-02 / IOS APPLICATION

Reviewed item	Scope	Recorded state
Evidence sample	12 account events	Email / booking reference retained
Control boundary	Diagnostic collection and export	Minimized, purpose-specific fields

Evidence register / Review window: 01-05 September 2026

E-02 - Reviewed record extract, September 2026.

Acceptance criterion

Repeat the reviewed user flows and verify that the diagnostic bundle excludes unnecessary personal identifiers.

Closure evidence to collect

1. Repeat the reviewed account and booking flows using profiles and inspect the resulting diagnostic export.
2. Verify email addresses and booking references are absent from unnecessary fields while correlation still supports diagnosis.
3. Retain the redacted schema comparison, build configuration and support access-policy review; do not attach unredacted logs to the report.

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.

Diagnostic allowlist

```
event.fields = ["event_name", "build", "correlation_id"]
// Email, booking reference and document contents are excluded.
```

References

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

OWASP Logging Cheat Sheet

Cached trip documents remain after sign-out

FINDING F-3	Medium / 4.6 / 10

Observation and affected context

The supplied local-storage inspection record shows two trip documents remaining in the application cache after sign-out.

Technical analysis

Sign-out ends the authenticated session but does not necessarily remove files created by document previews or offline features. The cache needs explicit account ownership and lifecycle rules. Operating-system cache eviction is opportunistic and should not be treated as an application sign-out control.

Affected scope and limits

Two trip documents remain in the before-and-after inventory. Persistence in the sandbox does not itself prove another application or a subsequent user can read them. The evidence establishes a retention mismatch; UI cross-account disclosure and privileged-device access remain unproven.

Impact

A later device user or a person with access to application storage may encounter data belonging to the previous session.

- Confidentiality: session-specific travel documents remain beyond the user's expected account boundary and could be exposed through a later access path.
- Account separation: reuse of cache keys or preview state could make cleanup failures more consequential. The assessment does not claim that such reuse was observed, and backend authorization is outside this scope.

Correction

Define a sign-out data-retention policy and remove session-specific cached documents while preserving only explicitly approved offline content.

1. Inventory session-specific files, preview artifacts, temporary exports and account-keyed caches. Distinguish explicitly approved offline content from material that must be removed.
2. Implement sign-out cleanup coordinated with in-flight downloads so a completed task cannot recreate a previous account's file after cleanup.
3. Use account-scoped cache keys and appropriate platform file protection. Remove stale references and preview state as well as files; document retention exceptions visibly to the user.

Accountable owner: Elise Laurent, mobile engineering lead. Preserve release and rollback evidence before requesting closure.

Supporting evidence

F-3 / Cached trip documents remain after sign-out

evidence record

E-03: before-and-after cache inventory for a account, 5 September 2026; two documents persist after sign-out.

E-03 / IOS APPLICATION

Reviewed item	Scope	Recorded state
Before sign-out	account cache	2 trip documents
After sign-out	Same cache inventory	2 documents remain

Evidence register / Review window: 01-05 September 2026

E-03 - Reviewed record extract, September 2026.

Acceptance criterion

Sign-out removes session-specific documents and switching accounts does not expose the previous account cache.

Closure evidence to collect

1. Compare sanitized cache inventories before and after sign-out for the same two documents.
2. Verify account switching and interrupted-download handling do not restore previous-account files or previews.
3. Confirm permitted offline features still work under the approved policy. File deletion is logical cleanup, not a claim of forensic secure erasure from flash storage.

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: 4.6 (Medium)
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/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.

Session cleanup contract

```
onSignOut:
  remove: [sessionDocuments, accountPreviews]
  preserve: [publicHelpContent]
  verifyAccountBoundary: true
```

References

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

OWASP MASVS-STORAGE-1 - secure storage

Remediation and retest

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

Action plan

F-1: Elise Laurent, mobile engineering lead. Target 30 September 2026. No personal trip details appear in app-switcher captures on either supported test device.

F-2: Elise Laurent, mobile engineering lead. Target 16 October 2026. Repeat the reviewed user flows and verify that the diagnostic bundle excludes unnecessary personal identifiers.

F-3: Elise Laurent, mobile engineering lead. Target 16 October 2026. Sign-out removes session-specific documents and switching accounts does not expose the previous account cache.

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.

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.