LOKI.
INTELLIGENCE

Loki Intelligence
Security Assessment Report

Security Assessment Report

Report for: Asteria Cloud public web estate

Professional summary of validated findings, affected assets, business risk, remediation priorities, retest criteria, and final security score.

Report classification

Fictionalized demo client report. Client names, domains, IP addresses, emails, screenshots, API keys, identifiers, raw request bodies, and evidence paths have been replaced with synthetic placeholders. The technical patterns, severity logic, remediation guidance, and reporting flow are based on sanitized Loki Intelligence assessment references.

Prepared by	Loki Intelligence
Client / target	Asteria Cloud, a fictional B2B SaaS company
Primary URL	https://www.asteria-cloud.example/
Validated surfaces	https://app.asteria-cloud.example/; https://api.asteria-cloud.example/; https://portal.asteria-cloud.example/
Assessment window	June 17-24, 2026

Executive Summary

Loki Intelligence assessed the public Asteria Cloud web estate, a fictional B2B SaaS environment with a marketing site, web application, API layer, desktop companion login bridge, customer portal, and OAuth/integration surface. The assessment identified six confirmed findings and five meaningful attack paths: one evidence-backed chain, three missing-link chains, and one rejected chain.

The highest-priority work is to bind the desktop companion login flow, reduce public workflow-schema exposure, suppress production traceback disclosure, and harden session, cookie, CORS, and logout behavior. The most important confirmed risk is not a proven breach. It is that future token exposure and anonymous reconnaissance become more valuable because the current controls allow additional auth material to be minted or implementation detail to be harvested.

The assessment did not prove account takeover, cross-account access, tenant compromise, admin access, billing or payment abuse, object data exposure, cloud or CI/CD compromise, third-party SaaS connector abuse, MCP tool abuse, or AI-tool compromise.

6	0	3	3	74 / 100
Confirmed findings	Critical / High	Medium	Low	Final security score

Risk area	Assessment result	Business meaning
Identity and session lifecycle	Moderate risk	The desktop token bridge and browser-session controls should be fixed before additional desktop or enterprise-login expansion.
Public workflow/API exposure	Moderate risk	Anonymous users can collect production workflow and implementation detail that improves targeted follow-up testing.
Browser security controls	Low to moderate risk	Current gaps are mostly pre-auth or disruption-focused, but several would become material if inherited by authenticated APIs.
Attack-chain resistance	Mixed	No broad compromise was proven, but one evidence-backed token chain and several missing-link chains require closure retests.

Severity note: CVSS v3.1 base scores are included for consistency. Loki business severity reflects validated blast radius, required preconditions, and whether the assessment proved data access or account takeover.

Scope And Methodology

Area	Details
Primary target	https://www.asteria-cloud.example/
Secondary validated surfaces	https://app.asteria-cloud.example/; https://api.asteria-cloud.example/; https://portal.asteria-cloud.example/; https://integrations.asteria-cloud.example/
Validated systems	Public website, workflow form runtime, JSON-RPC/API routes, app/session workflows, desktop companion login bridge, customer portal login, OAuth/integration metadata.
Testing mode	External assessment using controlled requests, test-owned accounts, browser validation, token/session lifecycle checks, and prior-phase evidence review.
Test accounts	Two test-owned customer accounts were used where authenticated validation was authorized. Credentials and identifiers are not included in this demo report.
Production safety	No destructive action, payment, fulfillment, persistence, irreversible state change, production submission, or delete effect was performed.
Limitations	Portal authenticated CORS reads, workflow backend submission, tenant-boundary checks, admin/support/billing workflows, native desktop traces, and object-level authorization require approved addenda.

Methodology

- Map externally exposed surfaces and group them by unauthenticated, authenticated customer, integration, and portal workflows.

- Validate findings with controlled request/response evidence, browser behavior, and repeatable variants rather than scanner output alone.

- Test attacker progression: anonymous discovery, malformed input, session/token lifecycle, cross-site browser behavior, OAuth/integration edge cases, and same-role account separation where safe accounts exist.

- Label unproven impacts as missing-link chains or addenda instead of inflating severity.

- Translate each confirmed capability into remediation guidance, acceptance criteria, detection needs, and retest steps.

Findings Overview

ID	Finding	Status	Severity	CVSS	Priority	Business meaning
FIND-001	Public workflow runtime and schema exposure	Confirmed	Medium	5.3	P1	Anonymous users can retrieve a public workflow runtime and JSON schema that include field names, hidden persistent fields, routing flags, and downstream workflow hints.
FIND-002	Desktop companion token bridge lifecycle weakness	Confirmed	Medium	5.4	P1	A fresh customer identity-provider token can be converted into additional same-account desktop/session material, and replay worked during the validation window.
FIND-003	Production JSON-RPC traceback disclosure	Confirmed	Medium	5.3	P1	Anonymous malformed JSON-RPC requests disclose production tracebacks containing source paths, custom module names, exception classes, and method signatures.
FIND-004	Session cookie issued over HTTP and missing explicit attributes	Confirmed	Low confirmed; conditional Medium	3.1	P1	Anonymous users receive session cookies before HTTPS is enforced, and cookie attributes do not consistently include Secure and explicit SameSite protections.
FIND-005	Cross-site logout and session clearing	Confirmed	Low business severity; CVSS Medium	4.3	P2	An unauthenticated web attacker can induce an authenticated browser to submit a cross-site logout POST and clear the application session.
FIND-006	Portal pre-auth CORS, cookie, and metadata hardening gaps	Confirmed	Low confirmed; conditional Medium	3.7	P2	The customer portal exposes pre-auth browser-policy and metadata weaknesses, including permissive sampled CORS behavior, incomplete cookie attributes, missing sampled HSTS, and version/API route metadata.

Highest-Risk Attack Paths

Chain ID	Status	Linked findings	Business outcome	Confidence	Priority
CHAIN-001	Evidence-backed chain	FIND-002	Increases impact of any future customer ID-token exposure by enabling same-account auth material minting and replay during the validation window.	Medium-high within valid-token precondition	P1
CHAIN-002	Systemic chain	FIND-001, FIND-003	Anonymous workflow schema exposure plus traceback detail improves targeted testing against workflow/API routes.	High	P1
CHAIN-003	Missing-link chain	FIND-004, FIND-005	Weak session/browser controls may support social-engineering timing or session confusion if a separate credential or auth-confusion path is proven.	High for primitives; low for downstream chain	P1/P2
CHAIN-004	Missing-link chain	FIND-006	Portal CORS and metadata gaps may become material if authenticated APIs inherit unsafe behavior.	Medium	P2 addendum
CHAIN-005	Rejected chain	OAuth/integration tests	No exploitable redirect, invalid-scope, silent-consent, state, or refresh-replay abuse was proven.	High rejection confidence	P3 hardening

Hard-Mode Coverage And Rejected Bypasses

Path or variant	Outcome	Reason / evidence	Priority
Public workflow runtime/config retrieval	Confirmed	Anonymous requests returned production workflow schema and hidden-field metadata. Evidence: EV-001.	P1
Workflow backend record creation or stored rendering	Not confirmed	No approved safe production submission object, staging route, or replay harness was available.	Addendum
Malformed JSON-RPC traceback disclosure	Confirmed	Anonymous malformed payloads returned production traceback detail. Evidence: EV-003.	P1
Desktop-login valid token across two test accounts	Confirmed	Token bridge accepted valid test-account tokens and returned same-account material. Evidence: EV-002.	P1
Desktop-login ID-token replay	Confirmed	Replay worked during the validation window. Evidence: EV-002.	P1
Desktop-login returned-token replay	Confirmed	Returned custom-token-like material replay worked during the validation window. Evidence: EV-002.	P1
Desktop-login missing or invalid token	Rejected	Requests without valid token material were rejected, constraining the confirmed issue to a valid-token precondition.	Context
Cross-site logout form POST	Confirmed	Authenticated test browser session was cleared. Evidence: EV-005.	P2
Logout GET/HEAD variants	Rejected	GET and HEAD did not reproduce the session-clearing behavior.	Context
Portal credentialed CORS customer-data read	Not confirmed	Pre-auth behavior was confirmed; authenticated API data-read impact requires approved portal test accounts.	Addendum
OAuth derived wildcard redirect	Rejected	Redirect_uri validation rejected derived wildcard-style callback abuse.	P3
OAuth invalid scope escalation	Rejected	Invalid or excessive requested scopes were rejected.	P3
OAuth consent/state/refresh replay	Rejected	Consent displayed requested scopes, callback state matched, and refresh replay failed.	P3

FIND-001 - Public Workflow Runtime And Schema Exposure

Status	Confirmed	Severity / priority	Medium / P1
CVSS v3.1	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	Confidence	High
Affected assets	https://www.asteria-cloud.example/; https://forms.asteria-cloud.example/; public onboarding workflow runtime	Owner	Web platform, workflow platform, backend API owner
Linked chains	CHAIN-002 systemic information-exposure chain	Evidence label	EV-001 sanitized evidence package

Executive summary

Anonymous users can retrieve a public workflow runtime and JSON schema that include field names, hidden persistent fields, routing flags, and downstream workflow hints.

Validated attacker capability

A remote unauthenticated user can load the public workflow page, identify the runtime configuration endpoint, and collect a complete client-side schema for the production onboarding workflow. No account, tenant membership, or API key is required.

Root cause

The client receives more workflow configuration than it needs to render the public form. Fields that should be server-owned, including queue routing and internal state flags, are exposed in browser-readable JSON.

Business impact

The exposure improves targeted testing for spam, replay, hidden-field overposting, file-upload abuse, stored rendering, and downstream workflow influence. Backend submission, staff-console impact, and stored cross-site scripting were not proven because destructive production submissions were out of scope.

Blast radius

Production workflow metadata across the public onboarding surface. No customer records, credentials, payment data, or tenant data were accessed.

Evidence observed

- EV-001-A: Anonymous GET request to the public workflow runtime returned browser-readable JSON configuration.

- EV-001-B: Extracted schema contained public input fields, hidden persistent fields, validation rules, and internal workflow names.

- EV-001-C: Submission and staff-rendering impact were intentionally not performed against production.

Reproduction summary

1. Request the public onboarding page from an unauthenticated browser session.

2. Identify the runtime configuration request in network traffic.

3. Fetch the JSON configuration directly without cookies or authorization headers.

4. Compare visible form fields against hidden persistent fields and server-side routing hints.

Recommended remediation

- Expose only the minimum schema required to render public form controls.

- Move hidden workflow, queue-routing, ETL, and staff-owned fields server-side.

- Enforce a server-side field allowlist and reject hidden-field overposting.

- Add replay protection, CSRF checks, rate limiting, and file-upload constraints.

- Validate staff/admin rendering with safe test-owned submissions before closure.

Acceptance criteria

- Unauthenticated clients can no longer retrieve internal workflow fields or routing metadata.

- Server rejects submitted fields that are not explicitly allowed for the public form.

- Safe replay, overposting, file-upload, and staff-rendering regression tests pass.

- Logs capture config-harvesting and rejected overposting attempts with request IDs.

FIND-002 - Desktop Companion Token Bridge Lifecycle Weakness

Status	Confirmed	Severity / priority	Medium / P1
CVSS v3.1	5.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)	Confidence	Medium-high within valid-token precondition
Affected assets	https://app.asteria-cloud.example/api/desktop-login; cloud identity-provider token exchange; desktop companion login	Owner	Identity platform, backend API owner, desktop app owner
Linked chains	CHAIN-001 evidence-backed chain; CHAIN-003 missing-link scenario if token acquisition is later proven	Evidence label	EV-002 sanitized evidence package

Executive summary

A fresh customer identity-provider token can be converted into additional same-account desktop/session material, and replay worked during the validation window.

Validated attacker capability

An attacker who already has a fresh valid customer ID token can submit it to the desktop-login bridge, receive custom-token-like material, exchange that material through the identity provider, and replay the original and returned token material during the tested window.

Root cause

The bridge accepted possession of a valid bearer token as sufficient authority. No evidence was observed for explicit desktop-flow state, nonce or device challenge, one-time code, PKCE-style binding, subject/session/device consistency checks, one-time issuance, or revocation-aware replay controls.

Business impact

A future transient token exposure becomes more valuable because it can be amplified into additional same-account auth material. This does not prove account takeover by itself, but it raises the impact of browser, desktop, log, extension, or endpoint token exposure.

Blast radius

Per compromised customer identity. The behavior was reproduced across two test-owned customer accounts. No cross-account, admin, tenant, billing, object-data, CI/CD, SaaS connector, MCP tool, or AI-tool reach was proven.

Evidence observed

- EV-002-A: Valid test-account token accepted by the desktop-login bridge.
- EV-002-B: Same ID-token replay accepted during the validation window.
- EV-002-C: Returned custom-token-like material replay accepted during the validation window.
- EV-002-D: Missing or invalid token requests were rejected, confirming the issue depends on a valid-token precondition.

Reproduction summary

1. Sign in with a test-owned customer identity and obtain a fresh ID token.
2. POST the token to /api/desktop-login without a desktop nonce, device challenge, or one-time code.
3. Exchange the returned token material through the configured identity-provider flow.
4. Replay the original ID token and returned material during the validation window.
5. Log out from the web app and retry the bridge with the still-fresh ID token.

Recommended remediation

- Require explicit desktop-flow state before minting desktop/session material.
- Use nonce, device challenge, one-time code, or PKCE-style binding for the native handoff.
- Enforce subject/session/device consistency, short lifetime, one-time issuance, and replay cache.
- Make logout, password change, account disablement, and token revocation invalidate bridge-created material.
- Log accepted and rejected attempts with subject, ambient session, content type, device, token age, replay result, and request ID.

Acceptance criteria

- Direct bearer-token bridge requests without valid desktop-flow state fail.
- Replays of the same ID token and returned material fail.
- Legitimate desktop login still succeeds through the intended bound flow.
- Logout, password change, account disablement, and provider revocation invalidate bridge-created material.

FIND-003 - Production Json-Rpc Traceback Disclosure

Status	Confirmed	Severity / priority	Medium / P1
CVSS v3.1	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	Confidence	High
Affected assets	https://www.asteria-cloud.example/api/jsonrpc; ERP-backed public website routes	Owner	Backend platform, ERP/CMS integration owner
Linked chains	CHAIN-002 systemic information-exposure chain	Evidence label	EV-003 sanitized evidence package

Executive summary

Anonymous malformed JSON-RPC requests disclose production tracebacks containing source paths, custom module names, exception classes, and method signatures.

Validated attacker capability

A remote unauthenticated user can trigger client-visible error responses that reveal implementation detail from production code paths. The finding does not require authentication and does not require high request volume.

Root cause

Production exception handling returns developer-oriented traceback detail to unauthenticated clients instead of a generic client-safe JSON-RPC error.

Business impact

The disclosure reduces attacker uncertainty for targeted route testing, module/advisory research, and schema-to-code correlation. No authorization bypass, data access, or code execution was proven.

Blast radius

Implementation metadata from the public website/API layer. No credentials, raw secrets, or customer data were returned in the validated evidence.

Evidence observed

- EV-003-A: Malformed JSON-RPC payload returned a production traceback to an anonymous client.
- EV-003-B: Traceback text exposed synthetic source-path placeholders, module names, exception classes, and method signatures.
- EV-003-C: Adjacent routes returned inconsistent error-handling behavior, suggesting missing regression coverage.

Reproduction summary

1. Send a malformed JSON-RPC request to the public API route from an unauthenticated session.
2. Confirm the response includes a traceback rather than a generic error envelope.

3. Extract exposed source-path, module, exception-class, and method-signature details.

4. Repeat against adjacent JSON-RPC routes to identify inconsistent handling.

Recommended remediation

- Disable client-visible production tracebacks for unauthenticated and authenticated users.
- Return generic JSON-RPC errors with stable request IDs.
- Log full exception detail server-side only.
- Review modules named in tracebacks for adjacent authorization and input-validation issues.
- Add malformed JSON regression tests across all public JSON-RPC routes.

Acceptance criteria

- Malformed JSON/JSON-RPC requests return generic client-safe errors.
- Full traceback detail is available only in server-side logs.
- Regression tests cover malformed body, wrong content type, missing params, and invalid method variants.
- Security logs include request ID, route, principal state, and sanitized exception class.

FIND-004 - Session Cookie Issued Over Http And Missing Explicit Attributes

Status	Confirmed	Severity / priority	Low confirmed; conditional Medium / P1
CVSS v3.1	3.1 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)	Confidence	High for anonymous routes; authenticated impact requires account retest
Affected assets	https://www.asteria-cloud.example/; http://www.asteria-cloud.example/; public session cookie behavior	Owner	Web platform, identity/session owner
Linked chains	CHAIN-003 missing-link session/browser-policy chain	Evidence label	EV-004 sanitized evidence package

Executive summary

Anonymous users receive session cookies before HTTPS is enforced, and cookie attributes do not consistently include Secure and explicit SameSite protections.

Validated attacker capability

A remote user can request the HTTP version of the site and observe a Set-Cookie response before canonical HTTPS redirection. HTTPS responses also showed inconsistent explicit browser protections during validation.

Root cause

The application/session middleware issues or refreshes session material before transport and browser-policy controls are applied consistently.

Business impact

The confirmed impact is weak anonymous session transport. The risk becomes materially higher if authenticated customer cookies inherit the same behavior or if sessions remain valid over HTTP.

Blast radius

Anonymous web sessions are confirmed. Authenticated session impact, logout/revocation behavior, stale-session handling, and account-bound impact require a test-account addendum.

Evidence observed

- EV-004-A: HTTP request received Set-Cookie before HTTPS enforcement.

- EV-004-B: Sampled session cookie lacked consistent Secure and explicit SameSite attributes.

- EV-004-C: Authenticated cookie behavior was not claimed because that path requires approved test accounts.

Reproduction summary

1. Request the HTTP canonical host with redirects disabled.

2. Inspect response order for Set-Cookie and Location headers.

3. Request the HTTPS canonical host and compare cookie attributes.

4. Verify whether anonymous and authenticated cookie policies are configured separately.

Recommended remediation

- Redirect HTTP to HTTPS before issuing any session cookie.
- Set Secure, HttpOnly, and explicit SameSite attributes on all session cookies.
- Enable HSTS on canonical HTTPS responses.
- Verify authenticated sessions cannot be used over HTTP.
- Confirm logout and session revocation invalidate session material consistently.

Acceptance criteria

- HTTP responses redirect to HTTPS without setting session cookies.
- All session cookies include Secure, HttpOnly, and an explicit SameSite value appropriate for the flow.
- Authenticated sessions are rejected over HTTP and stale sessions fail after logout/revocation.
- HSTS is enabled on canonical HTTPS responses after compatibility review.

FIND-005 - Cross-Site Logout And Session Clearing

Status	Confirmed	Severity / priority	Low business severity; CVSS Medium / P2
CVSS v3.1	4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L)	Confidence	High for forced logout; low for downstream phishing chain
Affected assets	https://app.asteria-cloud.example/api/logout; customer browser session cookie	Owner	Web platform, backend API owner, identity/session owner
Linked chains	CHAIN-003 missing-link social-engineering support chain	Evidence label	EV-005 sanitized evidence package

Executive summary

An unauthenticated web attacker can induce an authenticated browser to submit a cross-site logout POST and clear the application session.

Validated attacker capability

A victim who is signed in and visits attacker-controlled content can be forced to submit a cross-site form POST to the logout endpoint. The tested behavior clears the web session.

Root cause

The logout endpoint accepts a cross-site state-changing POST without evidence of CSRF token validation, Origin/Referer allowlisting, Fetch Metadata enforcement, or an equivalent same-site user-intent check.

Business impact

The standalone effect is session disruption, not data access. It may support phishing timing or auth-state confusion only if paired with a separate validated credential-capture, login-confusion, consent, or desktop prompt chain.

Blast radius

One victim browser session per interaction. No data access, privilege gain, tenant crossing, account takeover, or OAuth bypass was proven.

Evidence observed

- EV-005-A: Cross-site form POST to /api/logout cleared the test browser session.
- EV-005-B: GET and HEAD variants did not reproduce the session-clearing behavior.
- EV-005-C: No credential capture, consent phishing, or account takeover chain was validated.

Reproduction summary

1. Create an authenticated app session for a test-owned customer.
2. Serve attacker-origin HTML containing a POST form targeting /api/logout.

3. Load the page in the authenticated browser.

4. Confirm the endpoint returns success and the session cookie is removed.

Recommended remediation

- Protect logout with CSRF token validation, strict Origin/Referer allowlisting, Fetch Metadata policy, or an equivalent same-site intent requirement.

- Preserve legitimate same-site logout behavior.

- Reject form, text/plain, JSON, and attacker-Origin POSTs that do not satisfy the chosen control.

- Log denied attempts with cross-site request context.

Acceptance criteria

- Cross-site form and attacker-Origin POSTs no longer clear the session.

- Same-site UI logout still clears the cookie reliably.

- GET, HEAD, JSON, form, text/plain, missing Origin, and Fetch Metadata variants are covered.

- Alerts fire for cross-origin logout attempts and logout spikes.

FIND-006 - Portal Pre-Auth Cors, Cookie, And Metadata Hardening Gaps

Status	Confirmed	Severity / priority	Low confirmed; conditional Medium / P2
CVSS v3.1	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)	Confidence	Medium for pre-auth behavior; authenticated data impact not proven
Affected assets	https://portal.asteria-cloud.example/; pre-auth portal login and metadata routes	Owner	Customer portal owner, vendor integration owner, web platform
Linked chains	CHAIN-004 missing-link portal/API chain	Evidence label	EV-006 sanitized evidence package

Executive summary

The customer portal exposes pre-auth browser-policy and metadata weaknesses, including permissive sampled CORS behavior, incomplete cookie attributes, missing sampled HSTS, and version/API route metadata.

Validated attacker capability

Anonymous users can observe pre-auth portal metadata and browser-policy behavior that would make authenticated testing more precise. Credentialed cross-origin data reads were not proven.

Root cause

Portal defaults expose more pre-auth metadata than required and do not consistently enforce browser security headers across sampled responses.

Business impact

The confirmed impact is reconnaissance and hardening weakness. The risk becomes material if authenticated APIs inherit unsafe CORS behavior or if portal cookies are accepted in unsafe cross-origin contexts.

Blast radius

Pre-auth portal metadata and browser policy. Customer data exposure, tenant breakout, and portal account takeover were not proven.

Evidence observed

- EV-006-A: Pre-auth portal responses exposed version, customer, and API route metadata.
- EV-006-B: Sampled responses lacked consistent HSTS and cookie attributes.
- EV-006-C: Authenticated CORS data read was not claimed without approved portal test accounts.

Reproduction summary

1. Request portal login and metadata routes without authentication.

2. Send sampled requests with untrusted Origin and null Origin values.

3. Compare CORS, Set-Cookie, and HSTS behavior across login and API-adjacent routes.

4. Record exposed version, customer, and API route metadata.

Recommended remediation

- Restrict CORS to trusted origins, especially for authenticated APIs.

- Set Secure, HttpOnly, and appropriate SameSite on portal cookies.

- Enable HSTS on canonical HTTPS portal responses.

- Suppress unnecessary pre-auth version, customer, and API metadata.

- Coordinate vendor-managed configuration changes where the portal is externally managed.

Acceptance criteria

- Untrusted and null origins do not receive unsafe CORS behavior on sensitive routes.

- Authenticated APIs do not allow browser-readable cross-origin customer data from untrusted origins.

- Portal cookies consistently include Secure, HttpOnly, and appropriate SameSite attributes.

- Pre-auth portal metadata is minimized to operationally required content.

Rejected Or Not Confirmed Candidates

Candidate	Status	Reason	Residual risk
OAuth redirect/scope/refresh abuse	Rejected as exploitable	Wildcard-style redirect abuse, invalid scope escalation, missing-state concern, silent consent, and refresh replay were tested and rejected.	Keep dynamic-client-registration metadata policy tight and clean stale clients.
Workflow backend record creation or stored XSS	Not confirmed	No approved safe production submission object, staging path, or replay harness was available.	Needs staging or disposable test object before impact can be accepted or rejected.
Portal credentialed browser data read	Not confirmed	Pre-auth CORS behavior did not prove credentialed customer-data reads.	Needs two portal test accounts and approved object IDs.
Object/team/report/export authorization	Not confirmed / blocked	Safe persistent objects, elevated roles, and export data were not available for destructive or tenant-boundary checks.	Provision safe objects, teams, roles, and exports for addendum validation.
Cloud, CI/CD, SaaS connector, AI/tool compromise	Not confirmed	No validated evidence supports these impacts.	Continue normal secret, connector, and AI-tool review in future scoped phases.

Positive Security Observations

- OAuth redirect, invalid-scope, consent-state, and refresh replay abuse were rejected as exploitable in the tested configuration.

- Desktop-login requests without valid token material were rejected; the confirmed issue requires a valid fresh customer token.

- No broad systemic access-control failure, tenant compromise, admin access, billing/payment abuse, object data exposure, cloud compromise, CI/CD compromise, webhook compromise, MCP tool abuse, or AI-tool compromise was proven.

- Logout GET and HEAD variants were rejected; the confirmed logout issue was limited to cross-site POST behavior.

Remediation Roadmap

Timeline	Priority	Action	Primary closure evidence
0-7 days	P1	Bind /api/desktop-login to explicit desktop-flow state with nonce, device challenge, one-time code, or PKCE-style binding.	Original direct bearer-token bridge request fails; legitimate desktop flow works.
0-7 days	P1	Make bridge-created material one-time, short-lived, replay-resistant, and revocation-aware.	Replay attempts fail; logout, password change, account disablement, and provider revocation invalidate material.
0-7 days	P1	Remove or gate public workflow schema/config exposure and move hidden workflow fields server-side.	Unauthenticated config retrieval no longer exposes hidden fields; overposting tests fail safely.
0-7 days	P1	Disable production traceback disclosure for unauthenticated JSON/JSON-RPC requests.	Malformed payloads return generic errors with request IDs only.
0-14 days	P1	Enforce HTTPS before session issuance and set Secure, HttpOnly, and explicit SameSite attributes.	HTTP requests redirect without Set-Cookie; all sampled session cookies include expected attributes.
7-30 days	P2	Add CSRF, Origin/Referer, or Fetch Metadata enforcement for logout.	Cross-site form, JSON, text/plain, and attacker-Origin POSTs no longer clear sessions.
7-30 days	P2	Restrict portal CORS, enable HSTS, set secure cookie attributes, and suppress pre-auth metadata.	Untrusted origins receive no sensitive CORS behavior; portal metadata is minimized.
30-60 days	P2	Implement durable replay cache and anomaly detection for desktop-login.	Alerts fire on token reuse, returned-token replay, subject/session mismatch, and desktop-login after logout.
30-60 days	P2	Create session, CORS, traceback, workflow-schema, and token-lifecycle regression suites.	Automated tests run in CI and produce evidence for closure packages.
60-90 days	P3	Harden OAuth/MCP-style dynamic client metadata policy and clean stale test clients.	Redirect/scope/refresh controls remain strict; stale clients removed or reviewed.

Detection, Monitoring, And Retest Plan

Detection should turn the validated attack steps into observable events. For desktop-login, responders need enough fields to distinguish intended desktop use from bearer-token conversion and replay. For logout, responders need request context to distinguish user-initiated logout from cross-site session clearing. For workflow and JSON-RPC exposure, logs should separate routine errors from systematic harvesting.

Detection improvements

- Desktop-login logs: subject ID, ambient session ID, Origin, Referer, Fetch Metadata, content type, IP, user agent, device identifier, token age, revocation status, replay result, and request ID.

- Desktop-login alerts: same ID-token reuse, returned-token replay, subject/session mismatch, desktop-login after logout, suspicious content type, unusual user agent, and unusual device.

- Logout logs: actor/session ID, Origin, Referer, Fetch Metadata, source IP, user agent, content type, cookie-clearing result, same-site/cross-site classification, and request ID.

- Workflow/API logs: public config harvesting, rejected overposting, malformed JSON-RPC attempts, sanitized exception class, and correlation ID.

- Portal/OAuth logs: CORS policy violations, wildcard-looking redirect registrations, invalid scope requests, grant issuance, refresh rotation, replay failures, and stale client cleanup.

Retest and closure plan

ID	Retest objective	Expected fixed behavior	Closure evidence
FIND-001	Prove public workflow schema is minimized and overposting is blocked.	Hidden fields are absent from public config; submitted disallowed fields are rejected.	Request/response proof, schema diff, overposting logs.
FIND-002	Prove desktop-login requires bound flow state and rejects replay.	Direct unbound ID-token bridge and returned-token replay fail; legitimate desktop flow works.	Bridge transcripts, replay denial logs, revocation test artifacts.
FIND-003	Prove production tracebacks are not client-visible.	Malformed JSON-RPC returns generic error with request ID.	Before/after response proof and server-side log sample.
FIND-004	Prove session cookies are issued only after HTTPS enforcement and include attributes.	HTTP redirects without Set-Cookie; cookies include Secure, HttpOnly, and SameSite.	Header captures across anonymous and authenticated flows.
FIND-005	Prove cross-site logout no longer clears sessions.	Cross-site POSTs are denied or ignored; same-site logout works.	Browser cookie proof, request/response proof, alert/log evidence.
FIND-006	Prove portal CORS/cookie/header metadata is hardened.	Untrusted origins cannot read sensitive routes; pre-auth metadata minimized.	CORS/header captures and portal regression results.
CHAIN-001	Prove the token bridge chain is broken end to end.	Valid token alone is insufficient to mint desktop material; replay fails.	Chain retest transcript and log correlation.

Validation Addenda

Priority	Addendum	Why it matters	Evidence needed
P0	Native desktop login flow and product intent	Determines whether the desktop bridge is missing required device/challenge binding or matches intended design.	Native desktop trace, design notes, expected nonce/device/one-time-code behavior.
P0	Revocation lifecycle	Determines whether bridge-created material survives incident response actions.	Logout, password change, account disablement, and provider refresh-token revocation tests.
P0	Workflow safe submission validation	Determines whether schema exposure leads to backend record creation, hidden-field influence, or staff rendering impact.	Staging route or disposable test object, backend state proof, staff/admin rendering evidence.
P0	Portal authenticated CORS/API/object validation	Determines whether pre-auth portal hardening gaps affect customer data or tenant boundaries.	Two portal test accounts, object IDs, same-tenant and cross-tenant authorization evidence.
P1	OAuth/MCP-style tool-level authorization	Determines whether granted integration tools expose or mutate test-owned data unexpectedly.	Approved tool list, test-owned data, callback/replay harness, and tool-call logs.

Sanitized Evidence Index

Evidence ID	What it supports	Sanitization applied
EV-001	Public workflow runtime/config/schema exposure, hidden persistent fields, and route comparison.	Client names, domains, field values, identifiers, request IDs, and screenshots replaced with synthetic labels.
EV-002	Desktop-login token bridge validation, replay outcomes, valid-token precondition, and missing-token rejection.	Test account IDs, tokens, cookies, device identifiers, IPs, and raw JSON bodies removed.
EV-003	JSON-RPC traceback disclosure, source-path placeholders, module placeholders, exception classes, and method signatures.	Source paths and module names replaced with synthetic equivalents; no raw secrets included.
EV-004	HTTP/HTTPS session cookie behavior, missing attributes, and HSTS sampling.	Cookie values, host identifiers, IPs, and timestamps generalized.
EV-005	Cross-site logout/session clearing browser proof and rejected GET/HEAD variants.	Screenshots recreated as textual evidence labels; session IDs removed.
EV-006	Portal pre-auth CORS, cookie, HSTS, version, and metadata hardening gaps.	Vendor names, customer identifiers, route IDs, and screenshots replaced with placeholders.
EV-007	OAuth/integration rejected redirect/scope/state/refresh scenarios.	Client IDs, authorization codes, scopes beyond generic labels, and redirect identifiers removed.

Final Security Score

Asteria Cloud receives a final security score of 74/100 for this assessment. This is a moderate-risk result: no direct compromise was proven, but several externally exposed controls materially improve attacker precision or increase the value of future token/session exposure. The score should improve meaningfully after the P1 token bridge, schema exposure, traceback, and session-cookie fixes are closed with evidence.

Category	Score	Rationale
Identity and token lifecycle	68/100	Desktop-login bridge accepts valid bearer tokens without bound desktop-flow state and allowed replay during the validation window.
Web/API exposure control	71/100	Public schema exposure and traceback disclosure reveal actionable implementation detail without authentication.
Browser/session protections	69/100	HTTP cookie issuance, missing explicit cookie attributes, cross-site logout, and portal pre-auth CORS/header gaps require closure.
Authorization and blast-radius evidence	82/100	No account takeover, cross-account access, tenant compromise, admin access, or object data exposure was proven.
Detection and retest readiness	78/100	Findings have clear retest criteria, but telemetry needs more replay, cross-site, and schema-harvesting signals.
Overall	74/100	Moderate risk. Prioritize P1 fixes, then complete addendum validation with safe test data.

Closure statement

Closure requires evidence, not only a code merge. Each fix should include the original reproduction failing in the expected way, legitimate user-flow regression checks, security event evidence, and chain-interruption proof. Claims should remain limited to what retesting validates.