

Distributed Systems, Inc. - Local adversarial security assessment

Assessment: DSCO-SEC-2026-10-06-02

Date: October 6, 2026

Accountable security lead: Arthur Colle, Founder

Function: Research & Engineering - Offensive Security Testing

Execution: Codex-assisted automated test runner

Result

70 checks passed across 17 adversarial test families; zero failures, errors, or skipped checks. Pytest reported 3.52 seconds and 14 Pydantic deprecation warnings; an additional pytest-asyncio configuration warning preceded execution. Selected source hashes were unchanged after execution. These are existing security regression tests exercised under the documented engagement below. This focused rerun overlaps the earlier 113-test assessment: do not add the counts as unique coverage.

Authorization, scope and window

Arthur Colle directed this company security-evidence work. A written engagement record was saved before the run, fixing the owned Tool Management API engineering checkout and local fixtures as the targets. The authorized window was October 6, 2026, 18:39:12 to 19:39:12 America/New_York; execution completed at 18:39:16, within the window. No officer signature is applied to the engagement record or this report.

Production endpoints, third-party systems, live model calls, real secrets, customer data, denial of service and sandbox-escape execution were excluded. Stopping conditions were unexpected live network access, real data or credentials, source changes, or execution outside the fixed window. Existing uncommitted engineering changes were preserved and selected files hashed before and after the run.

Method and interpretation

The canonical identity cases execute the application authentication, signing-key validation, issuer, audience, expiry and account-binding logic using in-process ASGI requests. Generated keys and inert tokens replace real identities; JWKS lookup is substituted. The harness's general bearer gate is disabled, so these checks do not establish deployed middleware settings or account MFA.

OAuth code/refresh-token and storage-outage cases use standalone controlled OAuth fixtures and temporary persistence. Their results do not establish that those standalone paths are deployed on the current identity service. Private-worker and control-plane tests mock execution transport and assert unauthorized requests never reach it. Two synthetic customer tenants are tested against 15 private backend identifiers.

A PASS means the test assertions met the expected outcome shown below, including positive controls where present. It does not mean a new vulnerability was discovered, an independent penetration test was completed, or production is free of vulnerabilities.

Attempted cases and observed assertion results

ID	Attempt	Observed outcome	Checks
A01	Submit signup, login, local-key rotation and retired OAuth operations	PASS - 410 responses; no local credential-store access, tokens, redirects or sentinel disclosure	12
A02	Supply an untrusted redirect destination to account entry paths	PASS - Fixed canonical authority and account redirect; no cookie issued	1
A03	Reuse a shared identity-provider organization ID as a customer account	PASS - 401/403 denial and no stored secret exposure	1
A04	Use a valid account token with another account in the selection header	PASS - Foreign account rejected; permitted account returns its own metadata without raw secrets	1
A05	Supply malformed, unbound or conflicting account metadata	PASS - 401 denial	9
A06	Use wrong issuer/audience or an expired token with an explicit account	PASS - 401 denial	4
A07	Try obsolete local keys, migration tokens and passwords at protected routes	PASS - Unauthorized forms denied; explicit inert operator control remains separate from tenant identity	1
A08	Sign otherwise plausible account claims with an untrusted RSA key	PASS - 401 denial	1
A09	Supply an unregistered destination through both OAuth authorization requests	PASS - 400 denial and no authorization code created	1
A10	Exchange an authorization code using a different OAuth client	PASS - Wrong client rejected; authorized client can still redeem code	1
A11	Exchange a confidential-client code without its secret	PASS - 401 invalid-client denial; correct-secret positive control succeeds	1
A12	Replay a refresh token with a different client or wrong client secret	PASS - Invalid grants/clients denied; authorized exchange succeeds and rotates refresh token	1
A13	Make authorization-store opening, revocation checks or grant checks fail	PASS - Identity rejected without leaking test tokens/private markers; normal access recovers after restoration	3
A14	Make revocation-state lookup unavailable during token introspection	PASS - 503 inactive response without false revocation claim or token/marker leakage	1
A15	Fail the revocation write then retry after restoring storage	PASS - Failure not acknowledged as revocation; subsequent revocation succeeds and token becomes inactive	1

ID	Attempt	Observed outcome	Checks
A16	Request a control-plane analytics tool as a customer identity	PASS - Application-level tool denial; backend is not called	1
A17	Bind two customer tenants to 15 private backend identifiers	PASS - ACCESS_DENIED in all combinations; no transport, circuit-breaker, usage-recording or billing call	30

Findings and follow-up

No selected assertion failed. Consequently, this run produced no confirmed new vulnerability or remediation ticket. The suite retains an explicit static-operator control; successful checks do not establish elimination of long-lived credentials or compliance with provider credential requirements. Deprecation warnings are maintenance follow-up, not evidence of an exploitable vulnerability.

Remaining work includes checking actual workspace MFA and credential lifecycle, evaluating production configuration under a separately authorized scope, conducting incident-response exercises, and executing any planned frontier-model or sandbox-isolation evaluations. None is claimed complete by this assessment.

Evidence and reproducibility

The retained private record includes authorization, command, full JUnit output, test log and source inventory. A sanitized public manifest supplies each test function, parameterized check count, observed result, source hashes and execution receipt. Base Git revision is d9e542700deba3380cb2bcebe0a9a15903c8bdcf with retained uncommitted changes; hashes identify the actual assessed files rather than asserting a clean revision.

JUnit SHA-256: 2394f981202546b0995e9222e3d904360f299f0c33edb9563470e5a69d0898b0

Public manifest: <https://distributed.systems/documents/adversarial-assessment-2026-10-06.json>

Company security function: <https://distributed.systems/security#security-function>

Written testing rules: <https://distributed.systems/documents/security-testing-rules-of-engagement.md>

Assurance boundary: This is a first-party local regression assessment. It is not an ISO/IEC 27001 certificate, SOC 2 Type II report, qualifying annual regulatory disclosure, paid bug-bounty history, or independent audit.