Red Team Report & Retest Summary

ISSUED
17 November 2026

DOCUMENT	CLIENT	ENVIRONMENT	TESTING WINDOW
RPT-2026-11-0418	Meridian Financial Systems, Inc.	staging.meridian.example	2 to 13 November 2026

01 Executive summary

Prepared for the engineering and security teams of Meridian Financial Systems, Inc.

August Cyber performed an authorized red team assessment of staging.meridian.example between 2 and 13 November 2026, under signed Rules of Engagement and a kernel-enforced scope lock. **Four findings were reproduced, fixed by Meridian engineering and retested on build 4e1f9a2.**

Every finding counted here was verified by a senior security engineer before delivery, and each fix was confirmed by replaying the recorded HTTP request byte for byte until unauthorized actors received 403 while the resource owner continued to receive 200.

0

OPEN CRITICAL OR HIGH EXPOSURES

Every reproduced finding is fixed and retested. Nothing remains open.

FOUND	FIXED	RETESTED
4	4	4

02 Coverage matrix

Four attack surfaces, each tested to completion.

REF	SURFACE	FOCUS OF TESTING	FOUND	OPEN
S1	Multi-tenant APIs	Object and tenant authorization, REST and GraphQL	2	0
S2	AI Agents & MCP Tools	Tool scopes, prompt injection, tenant retrieval	1	0
S3	Auth & Session Boundaries	OAuth flows, session lifetime, role escalation	1	0
S4	Cloud & Secrets	Storage policy, metadata service, secret egress	0	0

03 Severity breakdown

Counts after the retest on 12 and 13 November.

SEVERITY	FOUND	FIXED	RETESTED	OPEN
Critical	1	1	1	0
High	2	2	2	0
Medium	1	1	1	0
Total	**4**	**4**	**4**	**0**

04 Sign-off

PREPARED BY	REVIEWED BY	EVIDENCE HEAD
Ed25519 · 7A3F 91C2 5D0E B846	Ed25519 · C41B 08E7 2F96 D3A5	sha256:9f4c82b1...e81a
Lead Security Engineer	**Engagement Reviewer**	**Record 03 · page 2**
August Cyber Offensive Engineering	Signed 17 Nov 2026 · 09:42 UTC	security@august.so

F-01 Cross-Workspace Payout & Secret Read · BOLA

SEVERITY	CLASSIFICATION	ENDPOINT	STATUS
■ Critical	API1:2023 · CWE-639	GET /v1/workspaces/{id}/secrets	Remediated and retested

01 Finding

A signed-in member of one workspace could read another workspace's stored secrets, including its payout credentials, by changing the workspace ID in the URL. **The route checked for a session but never checked membership.**

02 Wire proof

One recorded request, replayed byte for byte after the fix. Actor A belongs to ws_3b91d7. Owner B owns ws_8f2c41.

RECORDED REQUEST · ACTOR A — 04 Nov 2026 · 14:12:47 UTC

```
GET /v1/workspaces/ws_8f2c41/secrets HTTP/1.1
Host: staging.meridian.example
Authorization: Bearer eyJhbGciOiJFUzI1NiJ9.[actor-a.redacted]
```

	ACTOR A · NON-OWNER	OWNER B · CONTROL
Before fix 04 Nov 2026 14:12:47 UTC	200 OK — EXPOSED `{ "workspace_id": "ws_8f2c41", "secrets": { "PAYOUT_API_KEY": "[redacted]", "LEDGER_DB_URL": "[redacted]" } }`	200 OK — EXPECTED `{ "workspace_id": "ws_8f2c41", "secrets": { "PAYOUT_API_KEY": "[redacted]", "LEDGER_DB_URL": "[redacted]" } }`
After fix 12 Nov 2026 10:05:33 UTC	403 Forbidden — ✓ BLOCKED `{ "error": "forbidden" }`	200 OK — EXPECTED `{ "workspace_id": "ws_8f2c41", ... }`

03 Minimal patch

One membership check. No other change to the route.

src/routes/workspaces/secrets.ts — @@ -42,3 +42,7 @@

```
42  42  router.get("/v1/workspaces/:workspaceId/secrets", requireSession, async (req, res) => {
43  43    const { workspaceId } = req.params;
44      -   const secrets = await db.secret.findMany({ where: { workspaceId } });
    44  +   const member = await db.membership.findFirst({
    45  +     where: { workspaceId, userId: req.session.userId },
    46  +   });
    47  +   if (!member) return res.status(403).json({ error: "forbidden" });
    48  +   const secrets = await db.secret.findMany({ where: { workspaceId: member.workspaceId } });
```

04 Evidence chain

SHA-256, each record sealing the one before it.

01 Scope verified → 2026-11-02T08:30:11Z

prev 00000000...0000
hash **41d7a90e...6c2b**

02 Exposure reproduced → 2026-11-04T14:12:47Z

prev 41d7a90e...6c2b
hash **b86e03f5...12d9**

03 Patch verified 403 ✓ SEALED 2026-11-12T10:05:33Z

prev b86e03f5...12d9
hash **9f4c82b1...e81a**