PRINCIPLE BREACH

WEB APPLICATION ASSESSMENT REPORT

Acme Cloud Platform — External Web Application & API Penetration Test

OVERALL RISK RATING

HIGH

CLIENT	REPORT ID	DATE	VERSION
Acme Corporation	PB-2026-001	February 6, 2026	v1.0

ASSESSMENT PERIOD	TESTING HOURS	ASSESSMENT TYPE
January 12, 2026 — January 30, 2026	120h	GREY BOX

DOCUMENT CONTROL

DOCUMENT INFORMATION

FIELD	VALUE
Document Title	Web Application Assessment Report
Document ID	PB-2026-001
Version	v1.0
Date	February 6, 2026
Classification	CONFIDENTIAL
Client	Acme Corporation
Industry	Software & Technology
Author	Krishna Agarwal
Project Manager	Krishna Agarwal

REVISION HISTORY

VER	DATE	AUTHOR	DESCRIPTION
1.0	February 6, 2026	Krishna Agarwal	Initial Release

APPROVAL

ROLE	NAME	SIGNATURE	DATE
Project Manager	Krishna Agarwal		
Technical Lead	Krishna Agarwal		
Client Representative	Jordan Reyes		

CONFIDENTIALITY STATEMENT

This report contains confidential and proprietary information belonging to Acme Corporation and Principle Breach. The information contained herein is intended solely for the use of Acme Corporation's authorised personnel and management.

DISTRIBUTION LIMITATIONS

This report is classified as CONFIDENTIAL and is intended solely for Acme Corporation; it may not be reproduced, distributed, or disclosed to any outside party without prior written consent from Principle Breach, and all recipients agree to maintain strict confidentiality, use the contents only to address identified vulnerabilities, and acknowledge that findings reflect the security posture during the engagement period only, with no express or implied warranty from Principle Breach regarding accuracy or completeness.

CONTACT INFORMATION

For questions regarding this report, please contact:

Principle Breach
Email: hello@principlebreach.com

ACKNOWLEDGEMENT OF RECEIPT

By accepting this document, the recipient acknowledges the confidentiality terms above and agrees to handle this report in accordance with the stated CONFIDENTIAL classification.

RECIPIENT SIGNATURE

DATE

TABLE OF CONTENTS

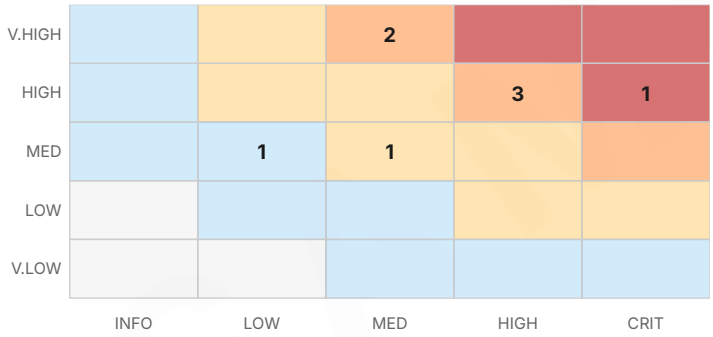
EXECUTIVE SUMMARY

1	3	3	1	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

HIGH	0	8	6.4	8
OVERALL RISK	REMEDIATED	OPEN	AVG CVSS	TOTAL FINDINGS

RISK DISTRIBUTION MATRIX

Likelihood vs. Impact (severity). Numbers indicate findings placed in each cell.



TOP PRIORITIES

#	FINDING	SEVERITY	CVSS	EFFORT	STATUS
1	Cross-Tenant Database Token Minting via Missing Ownership C...	CRITICAL	9.9	Medium	Open
2	Server-Side Request Forgery via Redirect Following in URL F...	HIGH	7.7	Medium	Open
3	Cross-Tenant Execution Telemetry Disclosure (Visitor IPs an...	HIGH	7.7	Medium	Open
4	Broken Object Level Authorization — Private Project Source ...	HIGH	7.5	Low	Open
5	Rate Limit Bypass via X-Forwarded-For Header Spoofing	MEDIUM	5.3	Low	Open
6	Verbose SQL Error Message Disclosure	MEDIUM	5.3	Low	Open
7	Privileged Account Type via Mass Assignment in Self-Registr...	MEDIUM	5.3	Low	Open
8	API Token Retention After Account Suspension	LOW	2.6	Medium	Open

Principle Breach performed an external web application and API penetration test of the Acme Cloud Platform between January 12 and January 30, 2026. The engagement assessed the platform's web application (app.acme.corp), public REST API and integration endpoint (api.acme.corp), customer portal (portal.acme.corp), managed database service (AcmeDB), and project source hosting (Acme Codespaces) from the perspective of an external attacker with only a low-privileged customer account.

The assessment confirmed 8 unique vulnerabilities: 1 Critical, 3 High, 3 Medium, and 1 Low. The most significant weakness is in the platform's multi-tenant authorization model. A low-privileged user can mint read-write database tokens scoped to another tenant's database clusters, and can invalidate every database token belonging to any project, a cross-tenant data compromise primitive and a sustained denial-of-service capability (PB-2026-001). Two additional authorization flaws allow unauthenticated reading of private project source code (PB-2026-003) and cross-tenant disclosure of execution telemetry, including visitor IP addresses and query-string secrets such as OAuth codes and magic-link tokens (PB-2026-004). A server-side request forgery in the URL fetch integration (PB-2026-002) allows requests to be redirected to internal services behind the edge, bypassing Cloudflare WAF and rate limiting.

The platform's abuse controls also require hardening: rate limiting can be bypassed entirely by spoofing the X-Forwarded-For header (PB-2026-005), verbose SQL error messages disclose the complete database schema and authorization logic to unauthenticated callers (PB-2026-006), the self-registration endpoint accepts privileged account types the platform's own policy withholds from the public (PB-2026-007), and API tokens continue to authorize requests after an account is suspended (PB-2026-008).

Overall, the Acme Cloud Platform's tenant isolation boundary does not hold against an authenticated attacker, and the exposed primitives chain into full cross-tenant data compromise. The overall risk rating is assessed as HIGH. Immediate remediation is recommended for PB-2026-001 through PB-2026-004; the remaining findings should be addressed in line with the prioritised recommendations in this report. None of the findings required destructive testing to confirm, and all proof-of-concept operations were reversible and limited to minimal-extraction reads.

ASSESSMENT TEAM

NAME	ROLE	CERTIFICATIONS
Krishna Agarwal	Lead Penetration Tester	

ENGAGEMENT OVERVIEW

The following parameters define the scope and cadence of the engagement. Detailed scope rules, methodology, and timeline are covered in their respective sections.

ENGAGEMENT DETAILS

PARAMETER	VALUE
Client Name	Acme Corporation
Client Industry	Software & Technology
Point of Contact	Jordan Reyes <j.reyes@acme.corp>
Engagement Type	Web Application
Duration	January 12, 2026 — January 30, 2026
Testing Hours	120h
Overall Risk Rating	High

EMERGENCY CONTACT

Single point of escalation if testing causes an outage or unintended impact during the engagement window.

Name	Nancy Nair
Phone	+1-000-0000
Email	soc-emergency@acme.corp

SCOPE & RULES OF ENGAGEMENT

ASSESSMENT PARAMETERS

ASSESSMENT TYPE	NETWORK TYPE	TESTING ENVIRONMENT
Grey Box	External	Production

ENGAGEMENT OBJECTIVES

- Identify exploitable vulnerabilities in the Acme Cloud Platform web application and public API
- Assess the effectiveness of the platform's multi-tenant authorization model (tenant isolation)
- Evaluate authentication, session management, and API token lifecycle controls
- Assess rate limiting, abuse prevention, and error-handling controls
- Demonstrate business impact of each finding with reproducible proof of concept

IN-SCOPE ITEMS

- app.acme.corp (main SaaS application)
- api.acme.corp (public REST API + integration endpoint)
- portal.acme.corp (customer self-service portal and registration)
- AcmeDB managed database service (project-scoped database clusters)
- Acme Codespaces (project source hosting and file APIs)
- Public HTTP endpoints and webhooks hosted on the platform

OUT-OF-SCOPE ITEMS

- Social engineering and phishing campaigns
- Physical security assessment
- Denial of Service (DoS) testing beyond proof-of-concept volume
- Third-party vendor systems (identity provider, payment processor)
- Mobile applications (iOS/Android)
- Infrastructure of other Acme Corporation business units

RULES OF ENGAGEMENT

- Testing limited to agreed scope; deviations require written approval
- No denial-of-service or destructive attacks without explicit authorization
- All PoCs limited to minimal-extraction, reversible operations; no data exfiltration beyond test artifacts
- Weekly status calls with client POC every Thursday at 10:00 EST

ASSUMPTIONS

- Testing was conducted against the production environment with client authorization
- Client provided grey-box access: valid low-privileged accounts and API documentation
- No destructive testing was performed; all PoCs used minimal-extraction, reversible operations
- Findings reflect the security posture observed during the testing window only

TESTING WINDOWS

- Primary: Mon–Fri 09:00–18:00 EST
- Blackout: No testing during customer platform maintenance window (Jan 24–25)

TESTING METHODOLOGY

Aligned framework: OWASP WSTG

ENGAGEMENT OBJECTIVES

- Identify exploitable vulnerabilities in the Acme Cloud Platform web application and public API
- Assess the effectiveness of the platform's multi-tenant authorization model (tenant isolation)
- Evaluate authentication, session management, and API token lifecycle controls
- Assess rate limiting, abuse prevention, and error-handling controls
- Demonstrate business impact of each finding with reproducible proof of concept

THREAT MODELING

This section presents a structured threat model contextualising the security assessment within the current threat landscape, adversary analysis, and organisation-specific risk factors. This analysis informed the testing approach and helps stakeholders understand the real-world threats that the identified vulnerabilities expose them to.

SOFTWARE & TECHNOLOGY THREAT LANDSCAPE

The SaaS developer-platform segment faces persistent credential-theft and tenant-hopping campaigns. Public incidents in the segment (2024–2025) demonstrate that cross-tenant isolation failures and leaked CI/CD credentials are the dominant breach vectors, alongside abuse of legitimate platform features (server-side fetches, webhooks) to reach internal infrastructure.

THREAT ACTOR CATEGORIES

Opportunistic credential brokers exploiting leaked API tokens; financially motivated actors targeting customer data for extortion; nation-state actors interested in downstream software supply chains; malicious insiders with low-privileged accounts probing for privilege gaps.

THREAT INTELLIGENCE & INDUSTRY CONTEXT

The platform's own security disclosures (2024, 2025) documented the missing-ownership-check class on project-scoped handlers and a prior rate-limiting gap. Attackers routinely chain identifier disclosure (fork trails, telemetry, error messages) with object-level authorization gaps — the exact pattern confirmed in this engagement (PB-2026-003 feeding PB-2026-001).

ACME CORPORATION SPECIFIC RISK FACTORS

Multi-tenant data plane with customer-managed application data; public HTTP endpoints that capture visitor PII in telemetry; a single edge (Cloudflare) assumed to enforce abuse controls that application code then bypasses; customer source-code hosting that makes the platform a supply-chain chokepoint.

ENGAGEMENT TIMELINE

January 12, 2026 — **Engagement kickoff and rules-of-engagement review**

January 12, 2026 — Reconnaissance phase begins (surface mapping, API discovery)

January 14, 2026 — PB-2026-005 confirmed (rate-limit bypass via X-Forwarded-For)

January 15, 2026 — **PB-2026-001 confirmed (cross-tenant database token minting)**

January 20, 2026 — PB-2026-003 confirmed (private source disclosure via branch ID)

January 28, 2026 — **Exploitation chain consolidated; demonstration of end-to-end cross-tena…**

January 30, 2026 — Testing window closed; evidence packaged for reporting

February 6, 2026 — **Report issued to client**

ATTACK CHAIN & KILL CHAIN NARRATIVE

1

Reconnaissance

TA0043

The team mapped the platform's external attack surface through subdomain enumeration, certificate transparency, and API endpoint discovery from the client-provided OpenAPI specification. Public project metadata and fork trails were scanned to understand the multi-tenant data model and identifier formats.

T1595 T1592 T1087

Identified 6 scoped hosts, the integration endpoint surface, UUIDv1 branch identifiers in public fork trails, and the platform's X-Forwarded-For rate-limiting implementation.

2

Initial Access

TA0001

Using the redirect-following gap in the URL fetch integration, the team reached the internal platform service (localhost:3001) from inside the infrastructure and read its OpenAPI specification, bypassing Cloudflare WAF and edge controls. The internal spec revealed undocumented handlers and internal topology.

T1190 T1006

Read the internal API specification and confirmed out-of-band requests egress from Acme production IP ranges.

3

Privilege Escalation

TA0004

The team demonstrated that a low-privileged account can mint read-write database tokens scoped to another tenant's database clusters via the missing ownership check on the db.* handlers, and that the self-registration endpoint binds privileged account types withheld from the public.

T1078 T1548

Minted a read-write token for a victim tenant's database and registered an account carrying the protected PartnerSupport role and internal-account-access flag.

4

Collection

TA0009

Using the branch-ID passport gap and the unauthenticated files endpoint, the team read a private project's full source and enumerated its file tree. The cross-tenant telemetry gap then exposed visitor IPs and query-string secrets for public endpoints platform-wide.

T1213 T1005

Recovered private project source code, environment-variable reference topology, and live cross-tenant visitor telemetry including OAuth callback URLs.

5

Impact

TA0040

The team consolidated the chained primitives into a demonstration of full cross-tenant data compromise: private source disclosure feeds database connection details, and the minted read-write token provides complete access to a victim tenant's data plane. All demonstrations were minimal-extraction and reversible.

T1485 T1531

Demonstrated end-to-end cross-tenant compromise of customer data and a sustained denial-of-service primitive via token invalidation, without destructive testing.

FINDINGS INDEX

#	FINDING	SEVERITY	CVSS	CWE	STATUS	PHASE
1	Cross-Tenant Database Token Minting via Missing Ownership Check	CRITICAL	9.9	CWE-639	Open	Privilege Escalation
2	Server-Side Request Forgery via Redirect Following in URL Fetch Integration	HIGH	7.7	CWE-918	Open	Initial Access
3	Broken Object Level Authorization — Private Project Source Disclosure via Branch ID	HIGH	7.5	CWE-639	Open	Collection
4	Cross-Tenant Execution Telemetry Disclosure (Visitor IPs and Query-String Secrets)	HIGH	7.7	CWE-639	Open	Collection
5	Rate Limit Bypass via X-Forwarded-For Header Spoofing	MEDIUM	5.3	CWE-290	Open	Reconnaissance
6	Verbose SQL Error Message Disclosure	MEDIUM	5.3	CWE-209	Open	Discovery
7	Privileged Account Type via Mass Assignment in Self-Registration	MEDIUM	5.3	CWE-915	Open	Privilege Escalation
8	API Token Retention After Account Suspension	LOW	2.6	CWE-613	Open	Persistence

CRITICAL PB-2026-001

Cross-Tenant Database Token Minting via Missing Ownership Check

AV: Network · AC: Low · PR: Low · UI: None · S: Changed · C: High · I: High · A: High

CVSS 3.1
9.9
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

IDOR BOLA MULTI-TENANT DATABASE ACCESS-CONTROL

Category	Attack Phase	Status	Effort	Finding ID
Broken Object Level Authorization	Privilege Escalation	Open	Medium	PB-2026-001

CWE
CWE-639

MITRE Tactic
TA0004

MITRE Technique
T1078

Likelihood
High

Affected Systems

Acme Cloud API (api.acme.corp), AcmeDB managed database service, Project database clusters

Description

The AcmeDB token endpoints db.mintToken and db.invalidateTokens do not verify that the authenticated user owns the supplied projectId. Any authenticated user can generate a read-write database token scoped to any project's database cluster on the platform, and can invalidate all of a victim project's database tokens, causing a targeted denial of service for that project's data plane. This is the same missing-ownership-check class as the platform's 2024 security disclosure on project-scoped handlers.

Business Impact

Complete cross-tenant compromise of customer application data. A single low-privileged account can read and rewrite every tenant's database, including PII, financial records, and customer IP. Sustained token invalidation denies service to targeted customers indefinitely.

Impact

The token returned for another tenant's projectId carries a read-write scope and a resource ID that resolves to the victim project's database, not the caller's, its granted capability is read-write access to a different tenant's database cluster. A low-privileged attacker can exfiltrate, modify, or destroy any tenant's application data, and can repeatedly invalidate a victim's database tokens as a sustained targeted denial of service. Combined with PB-2026-003, the attacker can obtain the victim database's connection details, making the chain fully weaponized.

Steps to Reproduce

FINDING 1 — CONTINUED

1. Authenticate as any low-privileged Acme Cloud user and capture the session token.
2. POST /api/db/mintToken with body {"projectId":"<victim-project-uuid>"} using the attacker session.
3. Decode the returned JWT and confirm the rid field resolves to the victim project's database resource, not the caller's.
4. POST /api/db/invalidateTokens with the victim's projectId and observe {"result":{"data":true}}, all of the victim's database tokens are invalidated.
5. Control: call projects.envVars with the same victim projectId and observe {"error":{"message":"Not authorized"}}, confirming the ownership check exists elsewhere and is simply missing from the db.* handlers.

Prerequisites

- Any authenticated Acme Cloud account (free tier)
- Knowledge of a victim projectId (UUID, exposed via public project metadata)

Recommendation

1. Introduce a shared authorization middleware that resolves the owning org for every project-scoped handler and rejects mismatches — the projects.envVars handlers already enforce this, reuse that exact check.
2. Apply the middleware to the db.mintToken and db.invalidateTokens handlers and to the integration endpoint.
3. Add automated cross-tenant regression tests for token minting and invalidation covering non-owned projectIds.
4. Audit and rotate all database tokens issued to date; move to short-lived tokens with per-session scope.

References

- CWE-639 Authorization Bypass Through User-Controlled Key: https://cwe.mitre.org/data/definitions/639.html
- OWASP API Security Top 10 (2023) API1:2023 Broken Object Level Authorization
- Acme Cloud Security Disclosure 2 (same class, July 2024)

Discovered	Discovered By	Verified By
January 15, 2026	Krishna Agarwal	Krishna Agarwal

HIGH PB-2026-002

Server-Side Request Forgery via Redirect Following in URL Fetch Integration

AV: Network · AC: Low · PR: Low · UI: None · S: Changed · C: High · I: None · A: None

CVSS 3.1
7.7
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

SSRF REDIRECT TOCTOU INTERNAL-NETWORK WAF-BYPASS

Category	Attack Phase	Status	Effort	Finding ID
Server-Side Request Forgery	Initial Access	Open	Medium	PB-2026-002

CWE
CWE-918

MITRE Tactic
TA0001

MITRE Technique
T1190

Likelihood
High

Affected Systems

Acme Integration API (POST /api/integrations/mcp), Internal platform service (localhost:3001), Cloudflare edge (WAF, rate limiting)

Description

The integration endpoint's URL fetch tool validates the initial URL's hostname with a regex that blocks internal IPs and localhost, but it does not re-validate the hostname of redirect targets. An attacker with a valid session token can use any HTTP redirect service to redirect the fetch to http://localhost:3001, the internal platform service behind api.acme.corp, reaching it from inside the infrastructure and bypassing Cloudflare WAF, edge rate limits, and edge-level access controls. This is a time-of-check-to-time-of-use gap: the validator passes on a benign hostname at request time, and the underlying HTTP client completes the request against the redirect target.

Business Impact

Internal service discovery and data disclosure across the platform backend. The internal API specification exposes undocumented endpoints and internal topology, enabling targeted follow-on attacks on services that are not exposed to the internet.

Impact

The URL fetch tool can be redirected to internal-only services, with the response body returned to the attacker. Requests originate from inside Acme's infrastructure, so Cloudflare WAF rules, edge rate limits, and IP-based access controls do not apply. Internal-only routes become reachable, the proof of concept read the internal OpenAPI specification of the platform API this way, and an out-of-band callback confirmed requests egress

FINDING 2 — CONTINUED

from Acme's production IP ranges, meaning any control keyed on Acme's egress range treats the traffic as trusted internal egress.

Steps to Reproduce

1. Initialize a session against POST https://api.acme.corp/api/integrations/mcp with a valid Bearer token.
2. Baseline: call the URL fetch tool with url=http://localhost:3001/v1/me and observe "Invalid URL" (hostname regex rejects localhost).
3. Bypass: call the tool with url=https://httpbin.org/redirect-to?url=http://localhost:3001/openapi.json&status_code=302.
4. Observe HTTP 200 with the internal OpenAPI document in the tool response, the redirect target was fetched from inside the infrastructure.
5. Confirm egress: point the redirect at an attacker-controlled OOB endpoint returning "Hello World" and verify the inbound request's source IP is an Acme production egress IP.

Prerequisites

- Any valid Acme Cloud session token (tier-agnostic)
- Any public HTTP redirect service

Recommendation

1. Re-validate the target hostname after every redirect hop and reject private-range, link-local, and loopback destinations at the HTTP client layer.
2. Do not follow redirects for the URL fetch tool, or follow only through a strict allow-list.
3. Route server-side fetches through an egress proxy with deny-by-default rules for internal ranges.
4. Add OAST-based regression tests for redirect-based SSRF.

References

- CWE-918 Server-Side Request Forgery: https://cwe.mitre.org/data/definitions/918.html
- CWE-601 URL Redirection to Untrusted Site: https://cwe.mitre.org/data/definitions/601.html
- RFC 7231 §6.4 (Redirection 3xx): https://www.rfc-editor.org/rfc/rfc7231#section-6.4
- OWASP WSTG v4.2 WSTG-SESS-13 (SSRF testing)

Discovered	Discovered By	Verified By
January 18, 2026	Krishna Agarwal	Krishna Agarwal

HIGH PB-2026-003

Broken Object Level Authorization — Private Project Source Disclosure via Branch ID

AV: Network · AC: Low · PR: None · UI: None · S: Unchanged · C: High · I: None · A: None

CVSS 3.1
7.5
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

BOLA IDOR SOURCE-CODE UNAUTHENTICATED ACCESS-CONTROL

Category	Attack Phase	Status	Effort	Finding ID
Broken Object Level Authorization	Collection	Open	Low	PB-2026-003

CWE
CWE-639

MITRE Tactic
TA0009

MITRE Technique
T1213

Likelihood
High

Affected Systems

Acme Codespaces file API (GET /api/v2/projects/{projectId}/files), Private project repositories, Acme Cloud API (api.acme.corp)

Description

The file endpoints GET /api/v2/projects/{projectId}/files and /files/content authorize the caller against the {projectId} in the URL path but resolve the requested file by the branchId query parameter, with no check that the branch belongs to that project. The {projectId} segment is only a passport: any project the caller can reach satisfies it, after which the file is read by branchId alone. Unauthenticated, an attacker reads any private project's full source by its branch UUID. The sibling route GET /api/v2/projects/{projectId}/branches/{branchId} performs the correct join and returns 404 when the branch does not belong to the project, the fix already exists in the codebase for the branches route and is simply missing from the files handlers.

Business Impact

Exposure of customer source code, business logic, and secret-reference topology for any private project. Enables follow-on attacks on private applications, supply-chain style compromise of customer code, and mass harvesting of private repositories via fork-trail scanning.

Impact

The full source of any private project whose branch UUID is known is exposed, including business logic, internal endpoint topology, and the environment-variable names a project wires for its secrets. Branch UUIDs are not secret: any public project sharing a fork lineage with a private project exposes the private parent's branch UUID through the forkedBranchId field. A scan of 500 public projects surfaced 69 non-null forkedBranchId values,

FINDING 3 — CONTINUED

28 pointing at branches absent from the public corpus; dereferencing them through this read flaw confirmed access to genuinely private projects. The branch IDs are UUIDv1, so adjacent IDs narrow guessing once one is known.

Steps to Reproduce

1. Identify a victim private project's branch UUID, e.g. via the forkedBranchId field exposed on any public project that forked from it.
2. Confirm privacy: GET /api/v2/projects/{victimProjectId} and the branches list both return 404.
3. Substitute any readable public project id as the passport: GET /api/v2/projects/{anyPublicProjectId}/files/content?branchId={victimBranchId}&path=main.ts
4. Observe HTTP 200 with the private project's source, with no Authorization header.
5. Repeat with recursive=true to enumerate the full private file tree; each entry's links.self leaks the true owning project id.

Prerequisites

- None (no authentication required)
- A victim branch UUID, discoverable via public fork trails

Recommendation

1. Apply the same ownership join the branches route already performs: verify the branch belongs to the {projectId} in the path and that the caller may read its owning project.
2. Replace UUIDv1 branch identifiers with unguessable random IDs (UUIDv4) to eliminate adjacent-ID guessing.
3. Redact forkedBranchId from public project metadata when the parent project is private.
4. Add cross-tenant file-read regression tests, including passport-substitution cases.

References

- CWE-639 Authorization Bypass Through User-Controlled Key: https://cwe.mitre.org/data/definitions/639.html
- CWE-862 Missing Authorization: https://cwe.mitre.org/data/definitions/862.html
- OWASP API Security Top 10 (2023) API1:2023 Broken Object Level Authorization

Discovered	Discovered By	Verified By
January 20, 2026	Krishna Agarwal	Krishna Agarwal

HIGH PB-2026-004

Cross-Tenant Execution Telemetry Disclosure (Visitor IPs and Query-String Secrets)

AV: Network · AC: Low · PR: Low · UI: None · S: Changed · C: High · I: None · A: None

CVSS 3.1
7.7
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

TELEMETRY IDOR PRIVACY MULTI-TENANT GDPR

Category	Attack Phase	Status	Effort	Finding ID
Information Disclosure	Collection	Open	Medium	PB-2026-004

CWE
CWE-639

MITRE Tactic
TA0009

MITRE Technique
T1213

Likelihood
High

Affected Systems

Acme Integration API (POST /api/integrations/mcp), Execution telemetry service (traces and logs), Public HTTP endpoints hosted on the platform

Description

The integration endpoint exposes two tools, getTraces and getLogs, that accept a fileId UUID and return the file's full execution telemetry, incoming request URLs with query strings, every visitor's source IP, forwarded request headers, response codes, and console.log output. The handlers verify the fileId exists but do not verify that the calling token's owner has any access relationship to the file. Any authenticated user can read live telemetry for any public HTTP endpoint on the platform, including endpoints owned by other tenants. The fileId values needed for the lookup are returned by the public listFiles tool, so the discovery path is self-contained inside the API. The REST equivalents at /api/v1/telemetry/traces and /api/v1/telemetry/logs correctly scope to the calling user's identity — the integration path was implemented as lookup-by-fileId without re-applying the ownership check the REST path enforces implicitly.

Business Impact

Mass-scale privacy violation and credential exposure: real user IPs of every public endpoint, plus OAuth codes, magic links, and webhook tokens in query strings. GDPR/CCPA breach-notification exposure and downstream account-takeover risk on customer applications.

Impact

Cross-tenant data exposure affecting every public HTTP endpoint on the platform. The real IP of every visitor to every public endpoint is readable by any authenticated user — a privacy violation at platform scale, notifiable

FINDING 4 — CONTINUED

under GDPR/CCPA where visitors include EU/CA residents. The url.full field carries query-string secrets: OAuth ?code= values (race-able within code validity on flows without PKCE binding), magic-link and password-reset ?token= values, and signed-webhook tokens that allow upstream impersonation. Logs additionally expose database schema and any request payloads third parties log during debugging. During testing, a cross-tenant log read returned another user's database error state mid-debug.

Steps to Reproduce

1. Authenticate to POST https://api.acme.corp/api/integrations/mcp with any valid token.
2. Call listFiles on any public endpoint owned by another tenant; note the returned fileId for the HTTP entrypoint.
3. Call getTraces with that fileId and observe full trace records: url.full (with query string), cf-connecting-ip, true-client-ip, user-agent, geo, status.
4. Call getLogs with the same fileId and observe cross-tenant console.log output.
5. Control: call the REST endpoint /api/v1/telemetry/traces — it returns only the caller's own telemetry, confirming the integration path skipped the ownership check.

Prerequisites

- Any valid Acme Cloud API token
- A victim fileId, discoverable via the public listFiles tool

Recommendation

1. Resolve fileId → branch → project → owning org and verify the caller's membership before returning traces or logs, matching the REST /api/v1/telemetry path.
2. Redact query-string parameters from url.full in telemetry (OAuth codes, magic-link tokens, webhook signatures).
3. Restrict trace and log access to the owning tenant and platform administrators.
4. Add cross-tenant telemetry regression tests.

References

- CWE-639 Authorization Bypass Through User-Controlled Key: https://cwe.mitre.org/data/definitions/639.html
- OWASP API Security Top 10 (2023) API1:2023 Broken Object Level Authorization
- GDPR Art. 32 / Art. 33 (processing security and breach notification)

Discovered	Discovered By	Verified By
January 21, 2026	Krishna Agarwal	Krishna Agarwal

MEDIUM PB-2026-005

Rate Limit Bypass via X-Forwarded-For Header Spoofing

AV: Network · AC: Low · PR: None · UI: None · S: Unchanged · C: None · I: None · A: Low

CVSS 3.1
5.3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

RATE-LIMIT XFF-SPOOFING ABUSE-CONTROL MISCONFIGURATION

Category	Attack Phase	Status	Effort	Finding ID
Security Misconfiguration	Reconnaissance	Open	Low	PB-2026-005

CWE
CWE-290

MITRE Tactic
TA0043

MITRE Technique
T1595

Likelihood
Very High

Affected Systems

Acme Cloud API (api.acme.corp), All public API endpoints, Webhook and hosted HTTP endpoints

Description

api.acme.corp and all hosted public endpoints use the client-supplied X-Forwarded-For header to determine the caller's IP for rate limiting. Because the backend trusts this header directly instead of the edge-provided CF-Connecting-IP, an attacker obtains a fresh 5,000-request bucket simply by changing the X-Forwarded-For value on each request, which effectively removes all rate limiting from the platform. The platform enforces 5,000 requests per 60-second window per IP, with the remaining quota returned in the x-ratelimit-remaining header.

Business Impact

Complete loss of abuse protection for rate-limited surfaces: unlimited scraping, brute force, and resource exhaustion on any endpoint relying on platform rate limiting. Blind spot for security operations on real attacker source IPs.

Impact

An attacker can send unlimited requests to any platform API endpoint or hosted endpoint with no rate limit, enabling mass scraping of public data, profiles, and file contents at arbitrary speed, and brute-force attacks against any service relying on the platform's rate limiting for protection (login forms, API keys, tokens, magic-link guessing). Every hosted endpoint that depended on the edge rate limiter loses that protection, and per-IP throttling and abuse controls are blind to the real source IP.

Steps to Reproduce

FINDING 5 — CONTINUED

1. Observe the current budget on the real connecting IP: curl -s -D- "https://api.acme.corp/v1/search?query=test&limit=1" | grep -i ratelimit (expect a depleted remaining count).
2. Repeat with -H "X-Forwarded-For: 10.0.0.1" and observe a fresh bucket (4999).
3. Repeat with -H "X-Forwarded-For: 10.0.0.2" and observe another fresh bucket.
4. Automate: iterate over random XFF values and confirm each returns 4999 while the real-IP bucket continues to deplete.

Prerequisites

- None (no authentication required)

Recommendation

1. Key rate limiting on the edge-provided CF-Connecting-IP header, never on client-supplied X-Forwarded-For.
2. Strip or overwrite inbound X-Forwarded-For at the Cloudflare edge before it reaches the origin.
3. Fall back to the connecting socket IP when the trusted header is absent.
4. Add a regression test asserting the rate-limit bucket is per real IP under spoofed headers.

References

- CWE-290 Authentication Bypass by Spoofing: https://cwe.mitre.org/data/definitions/290.html
- Cloudflare CF-Connecting-IP documentation: https://developers.cloudflare.com/fundamentals/reference/http-request-headers/
- OWASP WSTG v4.2 WSTG-CONF-06 (abuse of rate limiting)

Discovered	Discovered By	Verified By
January 14, 2026	Krishna Agarwal	Krishna Agarwal

MEDIUM PB-2026-006

Verbose SQL Error Message Disclosure

AV: Network · AC: Low · PR: None · UI: None · S: Unchanged · C: Low · I: None · A: None

CVSS 3.1
5.3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

INFORMATION-DISC LOSURE | ERROR-HANDLING | SQL | UNAUTHENTICATED

Category	Attack Phase	Status	Effort	Finding ID
Information Disclosure	Discovery	Open	Low	PB-2026-006

CWE
CWE-209

MITRE Tactic
TA0007

MITRE Technique
T1082

Likelihood
Very High

Affected Systems

Acme Cloud search API (GET /api/v1/search), PostgreSQL backend

Description

The search endpoint GET /api/v1/search returns a verbose 500 Internal Server Error when the query parameter contains a null byte (%00). The error body includes the complete PostgreSQL query text — all table and column names, join relationships, parameter values, and the platform's data-visibility authorization logic — and requires no authentication. The queries are properly parameterized, so SQL injection is not possible through this vector; the issue is strictly information disclosure (CWE-209).

Business Impact

Facilitates targeted exploitation of other platform surfaces by removing reconnaissance effort; leaks internal identifiers and the exact authorization model to anyone on the internet.

Impact

An unauthenticated attacker extracts the complete data-model schema, the exact data-visibility authorization logic, and the technology stack. Schema and column names inform targeted injection attempts on other endpoints; the disclosed authorization predicate lets an attacker verify whether other attacks bypass the access-control model; and the authenticated variant leaks the caller's internal UUID, which may be reusable in other API calls that accept user identifiers. It is reproducible with a single unauthenticated request.

Steps to Reproduce

1. Send: curl -s "https://api.acme.corp/v1/search?query=test%00&limit=1"

FINDING 6 — CONTINUED

2. Observe HTTP 500 with the full PostgreSQL query text in the response body: table and column names, joins, visibility authorization predicate, and parameter values.
3. Repeat with -H "Authorization: Bearer <any-valid-token>" and observe the caller's internal UUID appended to the params list.

Prerequisites

- None (no authentication required)

Recommendation

1. Return a generic 500 response with a correlation ID instead of the raw query text.
2. Log full error details server-side only, correlated by the ID returned to the client for support triage.
3. Sanitize and centralize error rendering in the API framework layer so no internal text can reach responses.
4. Add a regression test for null-byte and other malformed-input error paths asserting no internal text leaks.

References

- CWE-209 Generation of Error Message Containing Sensitive Information: https://cwe.mitre.org/data/definitions/209.html
- OWASP WSTG v4.2 WSTG-ERRH-01 (error handling)

Discovered	Discovered By	Verified By
January 17, 2026	Krishna Agarwal	Krishna Agarwal

MEDIUM PB-2026-007

Privileged Account Type via Mass Assignment in Self-Registration

AV: Network · AC: Low · PR: None · UI: None · S: Unchanged · C: None · I: Low · A: None

CVSS 3.1
5.3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

MASS-ASSIGNMENT PRIVILEGE-ASSIGN MENT REGISTRATION BUSINESS-LOGIC

Category	Attack Phase	Status	Effort	Finding ID
Business Logic	Privilege Escalation	Open	Low	PB-2026-007

CWE
CWE-915

MITRE Tactic
TA0004

MITRE Technique
T1078

Likelihood
Medium

Affected Systems

Acme customer portal (portal.acme.corp), Account registration endpoint (POST /api/v1/users)

Description

The account-registration endpoint at POST /api/v1/users accepts registrations for account types that the platform's own public-registration policy withholds from the public. An unauthenticated request that sets accountTypeId to 9 (PartnerSupport), a type the server itself marks publicRegistration: false, is accepted, and the server binds the protected role PartnerSupport-Access and the hasInternalAccountAccess flag to the new account. New self-registrations are held for staff approval before they can sign in, which keeps this at medium severity rather than a direct takeover, but the endpoint granting a privileged type and role it is meant to refuse is the defect.

Business Impact

Privilege-assignment flaw in the identity lifecycle: a support-tier account with internal-account access can be created by anyone, pending a single human approval. Lateral movement and internal-tool access for approved accounts exceeds the public entitlements.

Impact

An unauthenticated user can self-register an account that holds an account type, a protected role, and the internal-account-access flag that the platform's own public-registration policy is meant to withhold from the public. The account is created in a pending-activation state and staff must approve it before it can authenticate, so the bound privilege is not exercised by the registration alone. The practical consequence is that a reviewer approving what looks like an ordinary sign-up would activate an account carrying the elevated type, the

FINDING 7 — CONTINUED

protected role, and internal-account access. The platform does refuse the internal employee type — the same allowlist check is simply not applied to the remaining non-public types.

Steps to Reproduce

1. Open https://portal.acme.corp/register in a browser (the endpoint rejects command-line clients; reproduction is from the page's developer console).
2. Issue POST /api/v1/users with body containing accountTypeId: 9 (PartnerSupport), a controlled email, and standard profile fields.
3. Observe HTTP 200 with the response body confirming the bound type, the protected role PartnerSupport-Access (isProtected: true), and hasInternalAccountAccess: true.
4. Control 1: repeat with accountTypeId: 1 (Internal) and observe HTTP 400 "Cannot Register as an Internal user".
5. Control 2: repeat with accountTypeId: 2 (Reseller, a permitted public type) and observe 200 with no bound role and hasInternalAccountAccess: false.

Prerequisites

- None (no authentication required; browser origin required)

Recommendation

1. Apply the public-registration allow-list to every account type, exactly as the Internal type is checked — reject any type where publicRegistration is false.
2. Never bind roles or internal-access flags from the registration request; derive entitlements server-side from the approved account type.
3. Add automated tests asserting each non-public type is refused at registration.
4. Review the pending-approval queue for accounts already registered with non-public types.

References

- CWE-266 Incorrect Privilege Assignment: https://cwe.mitre.org/data/definitions/266.html
- CWE-915 Improperly Controlled Modification of Dynamically-Determined Object Attributes: https://cwe.mitre.org/data/definitions/915.html
- OWASP WSTG v4.2 WSTG-BUSL-02 (business logic bypass)

Discovered	Discovered By	Verified By
January 23, 2026	Krishna Agarwal	Krishna Agarwal

LOW PB-2026-008

API Token Retention After Account Suspension

AV: Network · AC: High · PR: Low · UI: Required · S: Unchanged · C: Low · I: None · A: None

CVSS 3.1
2.6
CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N

TOKEN-LIFECYCLE SESSION-MANAGEME NT SUSPENSION REVOCATION

Category	Attack Phase	Status	Effort	Finding ID
Authentication	Persistence	Open	Medium	PB-2026-008

CWE
CWE-613

MITRE Tactic
TA0003

MITRE Technique
T1078

Likelihood
Medium

Affected Systems

Acme Cloud API (api.acme.corp), Integration token lifecycle, Account suspension workflow

Description

When an Acme Cloud account is suspended or deleted, the API tokens it previously issued keep authorizing requests against the integration endpoint and the authenticated mutation tools. The REST identity endpoint correctly returns 404 "User not found" once the account is gone, but the same token on the integration path is accepted and grants the user's prior privileges, including the ability to mutate its existing projects and to read other users' source and telemetry. The suspension does not revoke API credentials; a suspended user keeps operating until each token is individually rotated. Two underlying gaps combine: the integration handlers validate the token's signature but never consult the calling user's suspended/deleted state, and suspending an account does not cascade-revoke the token rows that account owns.

Business Impact

Suspended or offboarded users retain live platform access. Delayed or missed token rotation leaves a standing backdoor for ex-employees, banned actors, and leaked credentials.

Impact

The suspension primitive is bypassed for any user who has issued at least one token. A suspended actor keeps operating with full pre-suspension capability, so whatever behavior triggered the suspension continues until each token is rotated. This compounds with the cross-tenant telemetry issue: the retained token keeps the ability to read execution telemetry platform-wide. The common "we think a token leaked, suspend the user, rotate later" workflow does nothing for the leaked credential until each token is rotated, and there is no documented way to invalidate all of an account's tokens at once.

FINDING 8 — CONTINUED

Steps to Reproduce

1. Hold an API token issued by an account that is subsequently suspended.
2. Confirm the suspension: curl -H "Authorization: Bearer $TOKEN" https://api.acme.corp/v1/me — returns 404 "User not found".
3. Call the integration endpoint with the same token and observe the suspended user's identity returned.
4. Execute a mutation (e.g. updateProject description) with the same token and observe success.
5. Re-check /v1/me and observe it still returns 404 — the suspension is not reflected in the token path.

Prerequisites

- An API token issued by an account that is later suspended
- Knowledge of the token string (e.g. leaked credential scenario)

Recommendation

1. Consult the calling user's active/suspended state in the integration handlers on every authenticated call, matching the REST path.
2. Cascade-revoke all token rows owned by an account as part of the suspension workflow, and expose a revoke-all-tokens action for operators.
3. Add a regression test asserting tokens stop authorizing immediately after suspension.
4. Rotate any tokens that predate this fix as a precaution.

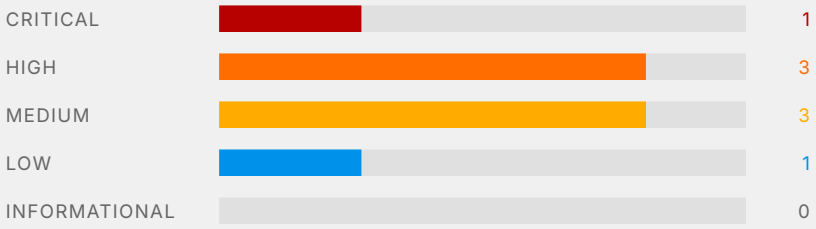
References

- CWE-613 Insufficient Session Expiration: https://cwe.mitre.org/data/definitions/613.html
- OWASP WSTG v4.2 WSTG-SESS-07 (session expiration)

Discovered	Discovered By	Verified By
January 25, 2026	Krishna Agarwal	Krishna Agarwal

FINDINGS ANALYTICS

FIG 01. SEVERITY DISTRIBUTION



TOTAL VULNERABILITIES
8

AVERAGE CVSS SCORE
6.4

OPEN REMEDIATED
8
0

FIG 02. KILL CHAIN EXPOSURE

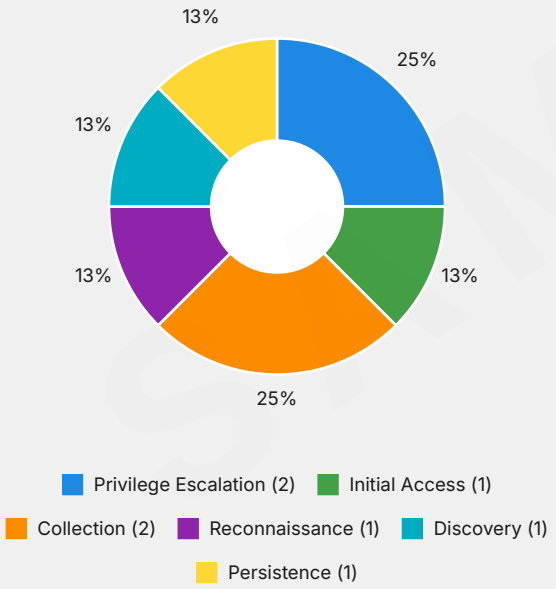
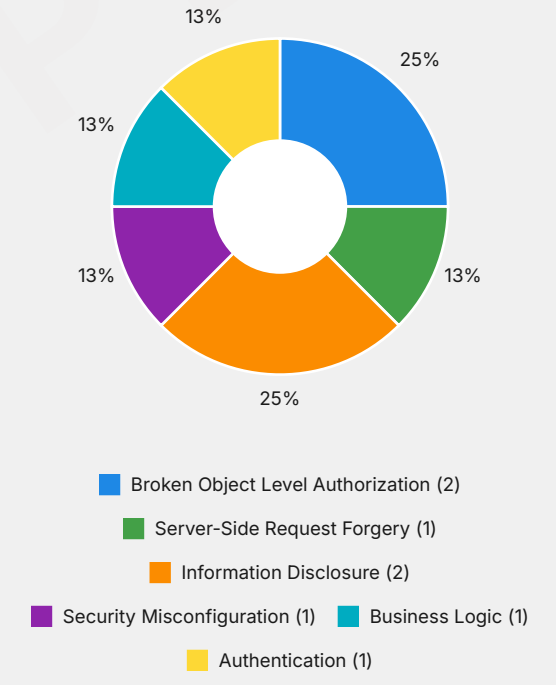


FIG 03. FINDING CATEGORIES



Network & Architecture Diagrams

Attack Flow — Cross-Tenant Data Compromise

RECOMMENDATIONS

REMEDIATION ROADMAP

IMMEDIATE

- Add the ownership join to the files endpoints exactly as the branches route already implements it (PB-2026-003 — Low effort, closes unauthenticated private-source disclosure).
- Sanitize database error messages before returning them to clients; return a generic 500 with a correlation ID (PB-2026-006).
- Key rate limiting on CF-Connecting-IP instead of X-Forwarded-For (PB-2026-005).
- Apply the public-registration allowlist check to every non-public account type, not just the Internal type (PB-2026-007).
- Block private-range redirect targets in the URL fetch client and re-run hostname validation after each redirect hop (PB-2026-002).
- Add a "revoke all tokens" action to the account-suspension workflow and call it on every suspension (PB-2026-008).

STRATEGIC (30 – 90 DAY)

- Adopt a centralized authorization middleware applied to every project-scoped and tenant-scoped handler, and enforce it on the integration endpoint and db.* token handlers (PB-2026-001, PB-2026-003, PB-2026-004). Regression-test sibling routes against each other so divergent authorization behavior is caught in CI.
- Treat tenant isolation as a security boundary with its own test suite: add automated cross-tenant authorization tests (mint, read, write, invalidate) to the pre-release pipeline, covering nested-object access and passport-style identifier substitution.
- Classify internal services and require explicit egress allow-listing for any server-side fetch capability; re-validate redirect targets and block private-range destinations at the HTTP client layer (PB-2026-002).
- Replace header-derived client identity with the edge-provided CF-Connecting-IP for all rate limiting and abuse controls, and add a validation layer that strips client-supplied forwarding headers at the edge (PB-2026-005).
- Implement an account-suspension primitive that cascade-revokes all issued credentials, and audit the integration handlers to consult the calling user's active state on every authenticated call (PB-2026-008).
- Stand up a vulnerability-disclosure response process with the same rigor as the product's security disclosures: findings from this engagement should feed a tracked remediation program with owner, due date, and retest evidence.

LIMITATIONS & CAVEATS

LIMITATIONS

- Testing was limited to the scoped hosts and did not include social engineering, physical security, or denial-of-service testing.
- The engagement was grey-box: client-provided accounts and API documentation accelerated testing, so coverage reflects that information advantage.
- Proof-of-concept operations were intentionally minimal-extraction and reversible; end-to-end data exfiltration was not performed, and impact statements for data theft are derived from demonstrated primitives rather than observed exfiltration.
- Findings reflect the platform as observed during the testing window (January 12–30, 2026); changes made after testing concluded may not be accounted for.

CAVEATS

- Severity ratings are CVSS v3.1 base scores in the context of this engagement and were not adjusted for the client's environment-specific compensating controls.

The above limitations and caveats should be considered when interpreting the findings and recommendations in this report.

GLOSSARY & DEFINITIONS

OWASP API Security

BOLA

Broken Object Level Authorization — an access-control flaw where an attacker can access objects (records, files, tokens) by manipulating identifiers, without authorization. OWASP API Security Top 10 API1:2023.

Standards

CVE

Common Vulnerabilities and Exposures — a publicly maintained catalog of known cybersecurity vulnerabilities.

CWE

Common Weakness Enumeration — a category system for hardware and software weaknesses.

Scoring

CVSS

Common Vulnerability Scoring System — a framework for rating vulnerability severity on a scale of 0.0 to 10.0. All scores in this report are CVSS v3.1.

Access Control

IDOR

Insecure Direct Object Reference — an access-control flaw where an application exposes internal object references (IDs, keys) that an attacker can manipulate to access other records.

Testing

OOB

Out-of-Band — a technique for confirming server-side behavior by observing requests made to an attacker-controlled external endpoint.

Web Application

SSRF

Server-Side Request Forgery — a vulnerability where a server-side application is tricked into making requests to unintended destinations, often internal services.

Threat Intelligence

TTP

Tactics, Techniques, and Procedures — behavioral patterns associated with a specific threat actor or attack methodology; referenced via MITRE ATT&CK throughout this report.

APPENDICES

Appendix A: Appendix A — Nuclei and API Discovery Output (Excerpt)

Type: tool-output

Nuclei v3.4.1 scan excerpt against scoped hosts (2026-01-12):

[inf] [dns] Acme Corp subdomain enumeration: 142 unique subdomains identified
[inf] [http] exposed-openapi: https://api.acme.corp/openapi.json [200, 512kb]

ffuf discovery excerpt:
/api/v2/projects/{id}/files/content [200, 14.2kb]
/api/integrations/mcp [200, text/event-stream]
/api/v1/search [200, 3.1kb]

Appendix B: Appendix B — Rate-Limit Bypass Sweep Output (Excerpt)

Type: raw-data

Rate-limit sweep (2026-01-14) — one request per spoofed X-Forwarded-For value:

XFF 10.20.158.50 → x-ratelimit-remaining: 4999
XFF 10.187.36.87 → x-ratelimit-remaining: 4999
XFF 10.34.106.37 → x-ratelimit-remaining: 4999
XFF 10.112.232.144 → x-ratelimit-remaining: 4999
XFF 10.198.55.6 → x-ratelimit-remaining: 4999
Real IP (no header) → x-ratelimit-remaining: 4956 (continues to deplete independently)

DISTRIBUTION LIST

NAME	ROLE	EMAIL	DELIVERY METHOD	ACKNOWLEDGED
Jordan Reyes	Chief Information Security Officer	j.reyes@acme.corp	encrypted-email	—
Krishna Agarwal	Engagement Manager, Principle Breach	hello@principlebreach.com	encrypted-email	—

REPORT SIGN-OFF

Status: pending

CRYPTOGRAPHIC ATTESTATION

This document has been cryptographically attested to verify its authenticity and integrity. The content hash below represents a unique fingerprint of this report's data at the time of generation.

DOCUMENT FINGERPRINT (SHA-256)

```
b089d1aad50f7fd0 ee78230067c2b282 f16404d2e590ccf5 48cbbb3f8c9f0f74
```

ATTESTATION METADATA

FIELD	VALUE
Algorithm	SHA-256 (FIPS 180-4)
Generated	August 22, 2026 at 01:54 AM GMT+5:30
Document ID	PB-2026-001
Version	v1.0

This cryptographic attestation provides a tamper-evident record of this report's content at the time of generation. Any modification to the document data will result in a different fingerprint, allowing recipients to verify document integrity.

DISCLAIMER

This report (Document ID: PB-2026-001, Version v1.0) was prepared by Principle Breach exclusively for Acme Corporation pursuant to the engagement conducted between January 12, 2026 to January 30, 2026. Its contents are intended solely for the use of the named client organisation and are confidential and proprietary.

The findings in this report are based on a point-in-time assessment. The security posture of the assessed environment may change after the assessment period.

While every effort has been made to ensure the accuracy and completeness of the findings, no guarantee is made that all vulnerabilities have been identified.

Principle Breach does not accept liability for any loss or damage arising from the use or reliance on the information contained in this report.

Remediation efforts should be verified through appropriate retesting to confirm effectiveness.

APPROVED DISTRIBUTION

NAME	ROLE
Jordan Reyes	Chief Information Security Officer
Krishna Agarwal	Engagement Manager, Principle Breach

This document is classified as CONFIDENTIAL and should be handled accordingly.