EXPOSUREMARK

External Exposure Assessment Report

CLIENT
Acme Technologies, Inc.

ASSESSMENT DATE
March 10–12, 2026

REPORT DATE
March 12, 2026

CLASSIFICATION
CONFIDENTIAL

REPORT ID
EM-2026-0312-ACME

SAMPLE REPORT — SANITIZED DATA

This report contains fabricated data for demonstration purposes. Actual assessments use real findings from your environment.

Contents

1. Executive Summary

OVERALL RISK	HIGH	Score: 72 / 100

INITIAL ACCESS	DATA ACCESS	ENV MAPPING
< 30 minutes	**< 1 hour**	**< 1 day**

SEVERITY	COUNT
Critical	2
High	4
Medium	7
Low	3

Assessment confidence: High. Based on full external visibility and manual validation of all critical findings.

Acme Technologies exposes 37 externally reachable assets across 3 domains and 2 cloud providers. 14 of these assets (38%) are not known to the internal team.

An unknown asset rate above ~15% typically indicates breakdowns in asset lifecycle management. At 38%, this is a systemic visibility gap — not isolated misses, but a structural failure in how external assets are tracked and governed.

These exposure patterns are consistent with what we observe across organizations of similar size and maturity.

Two critical findings provide direct, unauthenticated access paths to sensitive systems and data:

- **Administrative interface** accessible with default credentials on a non-inventoried server
- **Public API endpoint** exposing customer PII without authentication

Both are exploitable from the public internet with no prerequisites. This environment is currently exploitable without advanced techniques.

Estimated impact if exploited: full customer data exposure, unauthorized administrative access, regulatory implications (GDPR, CCPA), and high likelihood of credential reuse and lateral movement.

This level of exposure places the environment in a high-likelihood compromise category under standard threat models. No evidence of active exploitation was observed during the assessment window.

Immediate remediation of the two critical findings will materially reduce external risk. Remaining findings contribute to attack surface expansion and should be addressed in sequence. Detailed prioritization and ownership are provided in Section 10.

2. What Matters Right Now

This section provides decision-level prioritization for leadership and engineering.

Immediate — next 48 hours

- **EM-001:** Administrative panel with default credentials — direct database access
- **EM-002:** Unauthenticated API exposing customer data — active data exposure

These two issues provide direct access to sensitive systems and data. If only these are remediated, external breach risk drops significantly.

Short-term — next 30 days

- **EM-003:** Public S3 bucket — information disclosure, accelerates attack planning
- **EM-004:** Indexed staging environment — expands visible attack surface
- **EM-006:** Exposed .git repository — source code and credential exposure

These enable reconnaissance, accelerate attack path discovery, and reduce the effort required for exploitation.

Structural issue

38% of external assets are unknown to the internal team.

This indicates a breakdown in asset inventory and lifecycle management. Without addressing this, similar exposures will continue to reappear after remediation of current findings.

Everything else (EM-007 through EM-016) increases surface area but does not represent immediate breach risk. Address in sequence after the above.

3. Scope & Methodology

Scope

PARAMETER	VALUE
Primary domains	acmetech.com, acme-app.io
IP ranges	203.0.113.0/24, 198.51.100.0/28
Cloud providers	AWS (us-east-1), GCP (us-central1)
Exclusions	None
Assessment window	March 10–12, 2026 (72 hours)

Methodology

All reconnaissance and validation was conducted externally — no internal access, agents, or credentials were used.

- **Asset discovery** — DNS enumeration, certificate transparency logs, WHOIS, cloud metadata, search engine indexing, passive recon.
- **Service identification** — Port scanning, service fingerprinting, technology stack detection, API endpoint discovery.
- **Vulnerability assessment** — Manual validation against real exploitability, not theoretical CVSS scoring.
- **Attack path modeling** — Mapping how findings chain together to create viable attack sequences.
- **Compliance mapping** — Aligning findings to SOC 2 CC6/CC7, ISO 27001 A.12/A.13, PCI DSS Req. 2/6/11.

4. External Asset Inventory

37 assets identified — 23 previously known, 14 unknown to internal team (38%).

ASSET	TYPE	STATUS	KNOWN
acmetech.com	Domain	Active	Yes
www.acmetech.com	Subdomain	Active	Yes
api.acmetech.com	API endpoint	Active	Yes
staging.acmetech.com	Staging env	Active	No
old-admin.acmetech.com	Admin panel	Active	No
dev-api.acmetech.com	Dev API	Active	No
acme-app.io	Domain	Active	Yes
app.acme-app.io	Application	Active	Yes
203.0.113.47	Legacy service	Active	No
s3://acme-uploads-prod	S3 bucket	Misconfigured	No
s3://acme-backups-2024	S3 bucket	Public listing	No

Showing 11 of 37 assets. Full inventory in appendix.

5. Findings Summary

ID	SEV	FINDING	ASSET
EM-001	Critical	Admin panel with default credentials	old-admin.acmetech.com
EM-002	Critical	Unauthenticated API leaking customer PII	dev-api.acmetech.com
EM-003	High	S3 bucket with public listing enabled	s3://acme-backups-2024
EM-004	High	Staging environment indexed by Google	staging.acmetech.com
EM-005	High	TLS 1.0 enabled on production API	api.acmetech.com
EM-006	High	Exposed .git directory on web server	203.0.113.14

Showing 6 of 16 findings. Complete details in Section 7.

6. Why These Exposures Were Not Detected

The identified exposures are consistent with common gaps in external visibility:

- Assets discovered via certificate transparency logs and passive DNS are not tracked in internal inventory.
- Non-production systems (staging, dev, legacy) are externally reachable but not governed by the same controls as production.
- External reconnaissance is not part of regular security validation processes.
- Cloud resources and storage are created outside centralized governance.

These are structural issues rather than isolated misconfigurations. Addressing individual findings without fixing the underlying visibility and governance gaps will result in similar exposures reappearing.

7. Detailed Findings

EM-001	CRITICAL	Administrative panel with default credentials

Asset: old-admin.acmetech.com (203.0.113.47:8443)

DESCRIPTION

A Django administrative interface is exposed on port 8443 with default credentials (admin / admin123). This system is not present in the internal asset inventory. The interface provides direct access to application data, user management, and system configuration.

IMPACT

Full administrative access to backend systems. An attacker can access and export the user database (12,847 records), modify application behavior, create or escalate accounts, and extract API keys and configuration data. This represents immediate compromise of sensitive data and system control.

EVIDENCE

HTTP 200 response on /admin/ with successful authentication using default credentials. Database access confirmed with user records, billing metadata, and configuration data.

CONTEXT RELEVANCE

This finding combines two independent failures: (1) asset visibility failure — the system is externally exposed but not tracked internally, and (2) control failure — default credentials on an internet-facing administrative interface. This combination significantly increases risk, as the system is both unknown and unprotected. Findings of this type are consistently associated with rapid compromise during real-world attacks.

REMEDIATION

Immediately restrict access to this interface (IP allowlist or VPN). Remove default credentials and enforce strong authentication. Add system to asset inventory.

FOLLOW-UP

Assess whether this system should remain exposed or be decommissioned. Review all non-production and legacy systems for similar exposure patterns.

EM-002	CRITICAL	Unauthenticated API endpoint leaking customer PII

Asset: dev-api.acmetech.com/v1/users?format=json

DESCRIPTION

The development API is publicly accessible with no authentication. The /v1/users endpoint returns customer records including names, email addresses, phone numbers, and partial payment information. This appears to be a development instance running against production data.

IMPACT

Direct exposure of customer PII. Regulatory implications under GDPR, CCPA. Potential for credential stuffing using exposed email/password combinations. Rate limiting is not enforced, allowing bulk extraction.

EVIDENCE

GET request to endpoint returns JSON array with 500+ customer records per page. No authentication token required.

CONTEXT RELEVANCE

This is an environment isolation failure. Production data in a development environment without authentication represents both a data governance gap and an access control failure. This pattern is common in organizations where dev/staging environments are provisioned without security review.

REMEDIATION

Take this endpoint offline immediately. Review how production data reached a development environment. Implement authentication on all API endpoints. Notify legal/compliance team of data exposure.

FOLLOW-UP

Establish policy requiring synthetic data in non-production environments. Add API endpoint inventory to security review process.

EM-003	HIGH	**S3 bucket with public listing and partial read access**

Asset: s3://acme-backups-2024

DESCRIPTION

An S3 bucket containing database backups has public listing enabled. While individual objects require authentication, the listing reveals backup filenames including dates and database names.

IMPACT

Information disclosure about internal database structure, naming conventions, and backup schedule. Combined with other findings, this accelerates attack planning significantly.

EVIDENCE

aws s3 ls s3://acme-backups-2024 returns full directory listing. Files named: prod-db-2024-03-01.sql.gz, users-export-weekly.csv.gz, etc.

CONTEXT RELEVANCE

Cloud storage misconfigurations are among the most common findings in external assessments. This specific pattern — listing enabled, objects partially protected — creates a false sense of security. The information disclosed here (database names, backup schedules) directly aids an attacker planning access via other paths.

REMEDIATION

Remove public access. Apply bucket policy restricting to specific IAM roles. Enable S3 access logging. Review all buckets for similar misconfigurations.

Remaining findings (EM-004 through EM-016) follow the same structure in the full report.

8. Attack Path Analysis

Each path represents a realistic sequence an adversary could execute from the public internet using the identified findings.

Path 1: Staging → Admin → Database

STEP	ACTION	FINDING
1. Entry	Discover staging.acmetech.com via certificate transparency logs	EM-004
2. Pivot	Enumerate linked services, discover old-admin.acmetech.com	Recon
3. Access	Authenticate to admin panel with default credentials	EM-001
4. Objective	Export full user database (12,847 records) via admin interface	EM-001

Impact: Full database compromise. Time from initial discovery to data exfiltration: approximately 15 minutes. No specialized tooling required.

Why this path works: *Staging and admin systems are not isolated from each other or from the internet. Credential hygiene is not enforced on non-production systems. These are governance failures, not technical edge cases.*

Path 2: Dev API → PII Exposure → Credential Reuse

STEP	ACTION	FINDING
1. Entry	Discover dev-api.acmetech.com via DNS enumeration	Recon
2. Access	Query /v1/users endpoint — no authentication required	EM-002
3. Harvest	Extract customer emails, hashed passwords, partial payment data	EM-002
4. Escalate	Attempt credential stuffing against production login	EM-002 + EM-010

Impact: Mass PII exposure with regulatory consequences. Password hashes (bcrypt, low cost factor) are crackable within days for weak passwords. Combined with open redirect (EM-010), enables targeted phishing.

Why this path works: *Development environment uses production data without access controls. This is an environment isolation failure that creates a direct path from public internet to customer data.*

9. Compliance Readiness Map

Findings mapped to relevant control frameworks. This does not constitute a compliance audit — it identifies where external exposure creates control gaps.

FINDING	SOC 2	ISO 27001	PCI DSS
EM-001 Default credentials	CC6.1, CC6.3	A.9.4.3	Req. 2.1
EM-002 Unauth API	CC6.1, CC6.6	A.14.1.2	Req. 6.5.8
EM-003 Public S3 bucket	CC6.1	A.13.1.1	Req. 2.2
EM-004 Indexed staging	CC6.7	A.12.1.4	Req. 6.4.1
EM-005 TLS 1.0 enabled	CC6.7	A.10.1.1	Req. 4.1
EM-006 Exposed .git	CC6.1	A.9.4.1	Req. 6.3.2
EM-008 Zone transfer	CC6.6	A.13.1.1	Req. 1.1.6

Practical Implication

These findings would likely be flagged during SOC 2 audit under CC6 (logical and physical access) and CC7 (system operations), particularly due to publicly accessible administrative systems and unmonitored external assets.

The 38% unknown asset rate directly impacts ISO 27001 A.8 (asset management) and PCI DSS Requirement 2 (system configuration standards), as assets cannot be governed if they are not tracked.

Organizations preparing for SOC 2 Type II or ISO 27001 certification should treat these findings as pre-audit blockers rather than general risk items.

10. Remediation Plan

Immediate — within 48 hours

FINDING	ACTION	OWNER
EM-001	Restrict admin panel access (firewall/VPN). Change default credentials.	Infrastructure
EM-002	Take dev API offline. Audit production data in dev environments.	Engineering + Security
EM-003	Remove public access from S3 bucket. Audit all bucket policies.	Cloud/DevOps

Short-term — within 30 days

FINDING	ACTION	OWNER
EM-004	Remove staging from public DNS. Block search engine indexing.	Infrastructure
EM-005	Disable TLS 1.0/1.1. Enforce TLS 1.2+ on all endpoints.	Infrastructure
EM-006	Remove .git directory from web root. Add to deployment exclusions.	Engineering
EM-007	Implement CSP, HSTS, X-Frame-Options across all domains.	Engineering
EM-008	Restrict DNS zone transfers to authorized secondaries only.	Infrastructure

Structural — within 90 days

- Implement continuous external asset discovery (integrate with CI/CD and DNS management).
- Establish policy for staging/dev environment isolation — no production data in non-production environments.
- Deploy cloud security posture management (CSPM) for automated misconfiguration detection.
- Add external exposure review to quarterly security review cadence.
- Review and update asset inventory process — 38% unknown asset rate indicates systematic tracking failure.

11. Point-in-Time Limitations

This assessment represents a point-in-time snapshot of Acme Technologies' external attack surface as observed during the 72-hour assessment window (March 10–12, 2026). While it provides high-confidence findings validated by human analysts, it is important to understand what a single assessment cannot address.

What Changes Between Assessments

External attack surfaces are not static. Between the date of this report and the next assessment, the following changes are likely to occur without detection:

- **New assets appearing externally.** Development, staging, and cloud resources are regularly provisioned outside governance workflows. New subdomains, API endpoints, and cloud storage may become externally reachable at any time.
- **New vulnerabilities disclosed against your technology stack.** CVEs are published weekly against common frameworks, libraries, and services. Systems that were secure at assessment time may become exploitable as new vulnerabilities are disclosed.
- **Certificate and DNS changes.** Expired TLS certificates, DNS misconfigurations, and zone changes can introduce new exposure windows that did not exist during this assessment.
- **Credential exposure events.** Third-party breaches, dark web postings, and credential dumps containing employee or system credentials occur continuously and cannot be detected by periodic assessments.
- **Configuration drift.** Security configurations change through routine operations, deployments, and infrastructure updates. Remediated findings can reappear if underlying processes are not continuously validated.

Practical Implication

Organizations operating in environments similar to Acme Technologies typically experience measurable attack surface drift within 30–60 days of a point-in-time assessment. The structural visibility gap identified in this report (38% unknown assets) means that new exposures are likely to emerge through the same ungoverned channels that created the current findings.

Remediating the findings in this report addresses current risk. It does not prevent future exposures from occurring through the same structural gaps. Continuous external monitoring closes this window by detecting new assets, vulnerabilities, and configuration changes as they appear — rather than during the next scheduled assessment.

For organizations requiring continuous visibility — whether driven by insurance requirements, compliance obligations, or operational risk management — ExposureMark offers ongoing external risk monitoring services. Details are available at exposuremark.com or by contacting contact@exposuremark.com.

End of Report

ExposureMark · contact@exposuremark.com · New York Metro

How This Assessment Differs

This assessment identified 38% unknown assets and multiple viable attack paths from the public internet. These results are typical of what we observe across environments of similar maturity.

Automated EASM tools typically enumerate assets but do not validate exploitability, model chained attack scenarios, or provide the causal analysis needed to prevent recurrence.

Key differences in this assessment:

- **Manual validation** — every finding confirmed by offensive-certified operators, not algorithmic scoring
- **Attack path modeling** — findings chained into realistic adversary sequences with time-to-compromise estimates
- **Root cause analysis** — structural interpretation of why exposures exist, not just what they are
- **Decision-level output** — report structured for leadership action, not just technical documentation

For ongoing monitoring or follow-up assessment, contact contact@exposuremark.com.