Acme Financial Services - Security Incident Report

Prepared by: Alper Kandemir, Security Analyst

Date: 09 November 2025

Classification: Confidential

Executive Summary

This report details a coordinated, multi-vector **Security Incident** that impacted Acme Financial Services systems on **October 15, 2024**. The attack sequence was critically initiated by an **Account Compromise** of a privileged internal account, **admin_5678**, which successfully **exfiltrated** sensitive user data and proprietary documents via external channels. Immediately following this internal breach, an external threat actor (**203.0.113.45**) launched a simultaneous **Phishing Campaign** and destructive **SQL Injection (SQLi)** attempts against the web application.

The most critical finding is the **Horizontal Privilege Escalation** observed in the API layer, where multiple attackers utilized **stolen JWT (JSON Web Tokens)** to gain **Unauthorized Access** and enumerate **customer portfolio data**. The root causes are attributed to systemic security flaws: lack of **Multi-Factor Authentication (MFA)** for privileged accounts, insufficient **Input Validation** in the application layer, and a complete failure of **Resource-Level Authorization (Broken Access Control)** in the APIs. The overall impact is severe, confirming a **Loss of Confidentiality** for both customer and organizational data, mandating immediate reporting under compliance frameworks (**KVKK/GDPR**). Immediate containment and a strategic transition to a **Zero Trust** security model are mandatory.

Section 1: Incident Analysis (Condensed)

1.1 Timeline Reconstruction

The incident timeline on October 15, 2024, began with a critical internal event. At **08:55:00 UTC**, the internal IP address **10.0.1.50** used the **admin_5678** account to initiate a successful **User Data Exfiltration** via the administrative export function (HTTP 200 Response, web_logs.csv). Concurrently, at **08:55:12 UTC**, the same source IP was observed sending an email from **admin@acme.com** to an external ProtonMail address, attaching sensitive documents (email_logs.csv).

At **09:00:23 UTC**, the external attack commenced from **203.0.113.45**, initiating a **Phishing Campaign**. The same IP then attempted **SQLi** against /dashboard/search at **09:20:30 UTC**, aiming for **Database Destruction** (DROP TABLE users--) and **Data Theft**. The most significant proof of compromise is recorded in the API logs from **06:46:30 UTC** onwards, where **203.0.113.45** and other actors leveraged **Stolen JWTs** to access sequential, unauthorized portfolio IDs (api_logs.csv).

1.2 Attack Vector Identification

1.2.1 Phishing Campaign

The primary **Initial Access** vector utilized **Social Engineering**, spoofing **security@acme-finance.com** from **203.0.113.45**. The "URGENT" subject line sought to coerce users into surrendering credentials, facilitating the compromise of multiple user sessions.

1.2.2 SQL Injection Attack

The **SQLi** attempts, launched by **203.0.113.45** against the /dashboard/search endpoint, exploited a lack of **Input Validation**. The attempts to execute **DROP TABLE** confirm the attacker's intent for **Impact** and service degradation (waf_logs.csv).

1.2.3 Broken Access Control

API logs show attackers using compromised **JWTs** to perform **Horizontal Privilege Escalation** by modifying the resource ID. This demonstrates a critical absence of **Resource-Level Authorization** checks.

1.2.4 Data Exfiltration

The **Exfiltration** vector was directly linked to the internal IP **10.0.1.50** and the **admin_5678** account. The successful, unauthorized export of user data via the administrative panel, followed by external transfer of proprietary documents via unapproved channels, confirms a **Loss of Confidentiality**.

1.3 Attack Classification

Tactic	Technique	Description	Log Evidence
Initial Access	T1566.002 - Phishing: Spearphishing Link	Sending fraudulent email to deceive users.	email_logs.csv
Execution	T1190 - Exploit Public-Facing Application	Exploiting the web application vulnerability via SQLi.	waf_logs.csv
Persistence	T1078 - Valid Accounts	Using stolen JWT tokens for continued session access.	api_logs.csv
Credential Access	T1552 - Unsecured Credentials	Obtaining JWT tokens (likely via SQLi or Phishing).	api_logs.csv
Exfiltration	T1041 - Exfiltration Over C2 Channel	Extracting sensitive data (PDF) via external email.	email_logs.csv
Impact	T1499 - Endpoint Denial of Service (API)	Rapid sequential API attempts and enumeration on the API.	api_logs.csv

OWASP Top 10 2021 Mapping:

The incident maps to: A01:2021 - Broken Access Control (evidenced by Horizontal Privilege Escalation), A03:2021 - Injection (confirmed by SQLi exploitation due to lack of Input Validation), and A07:2021 - Identification and Authentication Failures (absence of MFA facilitated initial compromise and JWT theft).

1.4 Root Cause Analysis

The root causes are multi-layered:

1. **Fundamental Security Coding Flaws:** The core application lacked **Parameterized Queries** and robust **Input Validation**, rendering it inherently vulnerable to **SQLi**.
2. **Weak Access and Identity Management:** The absence of mandatory **MFA** for the **admin_5678** account made it susceptible to **Account Compromise**. The API failed to enforce **Resource-Level Authorization**.
3. **Lack of DLP and Behavior Monitoring:** The environment lacked **Data Loss Prevention (DLP)** controls to block mass **Data Exfiltration** to unapproved domains and possessed no **User and Entity Behavior Analytics (UEBA)** solution to flag the anomalous activity.

1.5 Impact Assessment

The impact is confirmed across multiple vectors:

- **Data Compromised:** Confirmed **Unauthorized Access** to **Customer Portfolio Data**, **Exfiltration** of the **entire User List Data**, confirmed loss of sensitive **Proprietary Documents**, and compromise of multiple active **JWTs**.
- **Business Impact:** The confirmed customer data loss will result in significant **Reputational Damage**. The SQLi attempts presented a serious **Operational Risk** of service downtime, and the targeting of **Transfer** and **Transaction** APIs indicates **Financial Risk**.
- **Compliance Impact:** The **Loss of Confidentiality** necessitates immediate **Breach Notification** to relevant Data Protection Authorities (Article 33 of **GDPR/KVKK**). Significant failures were observed in **ISO 27001** controls.

Section 2: Architecture Review (Condensed)

2.1 Current Architecture Weaknesses

The existing architecture is characterized by inadequate **Defense-in-Depth** and poor **Segmentation**.

- **API Security Gaps:** The lack of a dedicated **API Gateway** means there is no central **Policy Enforcement Point** for **Rate Limiting** or **Resource-Level Authorization**.
- **Network Segmentation Failure:** The **Internal IP 10.0.1.50** was able to initiate unauthorized exports and external email traffic, suggesting a flat internal network lacking stringent **egress filtering** for privileged hosts.
- **Reactive Perimeter:** The WAF lacked **Behavioral Analysis** capabilities to correlate the **Phishing** IP with the immediate **SQLi** attempts.
- **IAM Deficiency:** Critical administrator services were not secured with **MFA**.

2.2 Improved Security Architecture

[Reference to an **Improved Security Architecture Diagram** showing **API Gateway**, **Network Segmentation**, and **MFA** enforcement would be placed here.]

Key Improvements:

1. **API Gateway Implementation:** Deploy a dedicated **API Gateway** to centralize **Authentication**, **JWT Validation**, **Rate Limiting**, and enforce **Resource-Level Authorization**.
2. **Network Micro-Segmentation:** Isolate the internal network into distinct zones (e.g., **Admin Zone**, **Application Zone**, **Database Zone**). The **Admin Zone** must have the strictest **Egress Filtering**.
3. **Enhanced WAF & Cloud Security:** Integrate the WAF with **CSPM** using **Threat Intelligence** to automatically block known malicious IPs.
4. **Email Security Gateway:** Implement a robust solution enforcing **SPF/DKIM/DMARC** and providing advanced **Link/Content Sandboxing** to defeat **Phishing** and **Spoofing**.

2.3 Recommended Security Controls

Control	Justification (Addresses Vulnerability/Root Cause)
Input Validation & Parameterized Queries	Directly addresses the **SQLi** root cause (A03:2021) by ensuring data and code are treated separately.
Resource-Level Authorization	Fixes **Broken Access Control** (A01:2021) by verifying the **JWT**'s **user_id** claim against the requested resource.
Multi-Factor Authentication (MFA)	Mandatory for all privileged accounts to prevent unauthorized **Account Compromise** (T1078).
Data Loss Prevention (DLP)	Crucial to prevent unauthorized **Data Exfiltration** to external domains and block mass exports from sensitive interfaces.

2.4 Defense-in-Depth Strategy

The proposed strategy creates multiple security layers: **Network Layer** (Segmentation, WAF) prevents lateral movement; **Identity Layer** (MFA, Centralized IAM) ensures user trust; **Application Layer** (Parameterized Queries, Resource Authorization) protects data from exploitation; and the **Data Layer** (DLP) acts as a last line of defense.

Section 3: Response & Remediation (Condensed)

3.1 Immediate Actions (0-24 hours)

- **Containment & Revocation:** Immediately **Revoke** all **Compromised JWTs** and force password resets for all affected users (including **admin_5678**).
- **Blocking & Isolation:** Block all malicious **IOCs** (IPs: **203.0.113.45**, etc.) at the perimeter. Isolate the internal IP **10.0.1.50** and the associated machine for forensic analysis.
- **Forensics:** Create forensic images of the affected servers and log repositories.
- **Initial Notification:** Initiate the **Breach Notification** procedure under **GDPR/KVKK** guidelines.

3.2 Short-term Fixes (1-2 weeks)

- **Vulnerability Remediation:** Implement **Parameterized Queries** across all critical database interactions vulnerable to **SQLi**.
- **API Patching:** Deploy authorization middleware to enforce **Resource-Level Authorization** at API endpoints.
- **Credential Hardening:** Enforce **MFA** for all executive and privileged accounts.
- **Log Analysis:** Conduct a deep review of all historical logs associated with the **admin_5678** account.

3.3 Long-term Improvements (1-3 months)

- **Zero Trust Architecture:** Fully implement network **Micro-Segmentation** and deploy a central **API Gateway**.
- **Security Monitoring:** Deploy a **SIEM** solution with **UEBA** capabilities to detect anomalies in real-time.

- **SDLC Integration:** Implement mandatory **Secure Code Review** and automated **SAST/DAST** tools to prevent future **SQLi** and **Broken Access Control** vulnerabilities.
- **User Training:** Conduct mandatory, updated **Social Engineering/Phishing Awareness Training** for all personnel.

3.4 Compliance Considerations

The confirmed data loss requires compliance with **GDPR / KVKK**, specifically **Article 33 (Breach Notification)** and **Article 32 (Security of processing)**. Remediation addresses gaps in **ISO 27001 Controls** (A.9.4.2 via MFA, A.14.2.1 via code review, and A.18.1.3 via DLP). The long-term plan is structured around the five functions of the **NIST Cybersecurity Framework**.

Conclusion

This incident demonstrates the critical consequence of fragmented security controls and the importance of a **Defense-in-Depth** strategy. The coordinated **multi-vector attack** exploited failures across the Identity, Application, and Network layers. The immediate and long-term implementation of the recommended controls, focusing on **MFA**, **Resource-Level Authorization**, and **Network Segmentation**, is paramount to restoring trust and establishing a resilient security posture.

Appendix A: Log Evidence

- **Data Exfiltration:** web_logs.csv (line 2: 2024-10-15 08:55:00, **admin_5678**, /admin/users/export, 200, 15673, **10.0.1.50**)
- **SQLi Attempt:** waf_logs.csv (line 3: 2024-10-15 09:21:15, CRITICAL_BLOCK, **203.0.113.45**, /dashboard/search, **SQL Injection - DROP TABLE**)
- **Broken Access Control:** api_logs.csv (line 27: 2024-10-15 06:47:33, 1523, /api/v1/portfolio/1533, **203.0.113.45**, **jwt_token_1523_stolen**)
- **Phishing & External Transfer:** email_logs.csv (line 2: 2024-10-15 08:55:12, admin@acme.com, **external.contact@protonmail.com**, **10.0.1.50**)

Appendix B: IOCs (Indicators of Compromise)

- **IP Addresses (Block Immediately):**
  - **203.0.113.45** - Malicious attacker IP
  - **10.0.1.50** - Internal IP associated with **Data Exfiltration**
  - **98.213.45.122** - Secondary external attacker
  - **172.89.15.67** - Secondary external attacker
- **Compromised Session/User IDs (Revoke Access Immediately):**
  - **jwt_token_1523_stolen**
  - **jwt_token_2347_abc**
  - **jwt_token_3891_def**
  - **admin_5678** - Internal Admin account
- **External Resources:**
  - **security@acme-finance.com** - Spoofed Phishing Sender
  - **external.contact@protonmail.com** - Data Exfiltration Destination