# Incident Report: Zero-Day Exploit Attack on Acme Tech

## Date of Incident:

April 5, 2025

## Reported By:

Jane Smith, Lead Security Analyst

## Incident Type:

Zero-Day Exploit

## Incident Severity:

Critical

## 1. Summary of the Incident

On April 5, 2025, at 11:20 AM UTC, Acme Tech detected unauthorized access to internal web applications, traced back to an unknown exploit in the latest version of their enterprise web server. Attackers leveraged a zero-day vulnerability (CVE-2025-XXXX) to gain remote code execution (RCE), allowing them to install backdoors and exfiltrate sensitive customer data. The breach was identified when SIEM flagged suspicious outbound traffic from the application server to an unrecognized external IP.

Incident Response (IR) was activated at 11:40 AM, and mitigation efforts began. All affected systems were isolated, and forensic analysis confirmed the exploitation of an unpatched vulnerability. A security patch was deployed once a fix became available, and additional security measures were implemented to prevent further attacks.

## 2. Incident Detection and Response Timeline

|  |  |
| --- | --- |
| Time (UTC) | Event |
| 11:20 AM | SIEM detects unusual outbound traffic from internal application server. |
| 11:30 AM | SOC investigates and finds unauthorized shell access on the server. |
| 11:40 AM | Incident Response Team activated, affected servers isolated. |
| 12:00 PM | Threat intelligence confirms exploitation of a zero-day vulnerability (CVE-2025-XXXX). |
| 12:30 PM | SOC identifies indicators of compromise (IoCs) and blocks malicious IPs. |
| 01:15 PM | Security team deploys a temporary mitigation measure. |
| 02:00 PM | Third-party vendor confirms the zero-day exploit, and emergency patch development begins. |
| 04:30 PM | Security patch released; patching and system restoration begin. |
| 06:00 PM | Post-incident forensic analysis initiated. |
| 07:30 PM | Security monitoring enhanced, incident report drafted. |

## 3. Impact Assessment

Affected Systems: Enterprise web servers, API gateway, customer data storage.

Downtime: Approximately 6 hours.

Data Compromised: Potentially 10,000 customer records.

Financial Impact: Estimated $500,000 in damages and regulatory fines.

## 4. Root Cause Analysis

Entry Point: Zero-day vulnerability in proprietary web application.

Attack Vector: Remote Code Execution (RCE) via unpatched flaw.

Security Gaps: Lack of virtual patching mechanism, delayed detection of anomaly.

## 5. Containment and Mitigation Actions

Isolated compromised servers and revoked all active sessions.

Applied temporary virtual patch via Web Application Firewall (WAF).

Blocked malicious IPs and reinforced access control policies.

## 6. Lessons Learned & Preventative Measures

Enhance Zero-Day monitoring with threat intelligence feeds.

Deploy an automated virtual patching mechanism for known vulnerabilities.

Strengthen SIEM correlation rules to detect anomalous behavior faster.

## 7. Conclusion

This zero-day attack exploited an unknown vulnerability, reinforcing the need for proactive security monitoring and rapid response capabilities. Future security efforts should focus on minimizing the attack surface, strengthening security patching strategies, and improving threat intelligence integrations.