Root Cause Analysis Report

Gotham City Police Department - IT Security Division

Document Number: RCA-2024-112

Date: 11/17/2024

Incident Title: Unauthorized Access to GCPD Criminal Database
Ticket Number: INC5528

Classification: CONFIDENTIAL

Contents

1 Executive Summary

- **Incident Date:** November 14, 2024, 02:13 EST
- **Incident Location:** GCPD Main Data Center
- **Duration:** 47 minutes of unauthorized access
- **Impact:** Unauthorized access to Level 3 criminal records and ongoing investigation data
- **Root Cause:** Exploitation of legacy authentication system using credentials from decommissioned terminal in evidence room B-13
- **Key Recommendations:** Implementation of zero-trust architecture and complete decommissioning of legacy authentication systems

2 Incident Description

2.1 Background

At 02:13 EST on November 14, 2024, our security monitoring systems detected anomalous access patterns to the GCPD Criminal Database (GCDB). The access originated from a decommissioned terminal in evidence room B-13, which was supposed to have been disconnected from the network during the previous quarter's infrastructure upgrade. Subsequent investigation revealed that the terminal was remotely accessed using Commissioner Gordon's old credentials, which had not been properly invalidated in the legacy authentication system.

2.2 Timeline of Events

Date/Time	Event Description
11/14/24 02:13	Initial unauthorized access detected from evidence room B-13 terminal
11/14/24 02:15	SIEM alerts triggered for anomalous data access patterns
11/14/24 02:17	Automated security response initiated, blocking external data transfers
11/14/24 02:20	SOC team began initial investigation
11/14/24 02:25	Discovery of active session using Commissioner's legacy credentials
11/14/24 02:30	Physical security dispatched to evidence room B-13

11/14/24 02:35	Batman encountered in evidence room, claimed investigating Penguin case
11/14/24 02:45	Initial damage assessment begun
11/14/24 03:00	All legacy authentication systems taken offline
11/14/24 03:30	System access restored with enhanced monitoring

3 Investigation Team

Name	**Role**	**Department**
Barbara Gordon	Lead Security Analyst	GCPD Cybersecurity
Lucius Fox	Security Consultant	Wayne Enterprises
Dick Grayson	Network Engineer	GCPD IT Infrastructure
Timothy Drake	Forensics Specialist	Digital Forensics Unit

4 Analysis Methods Used

- Log analysis using Splunk Enterprise Security
- Network traffic analysis using Wireshark
- Forensic analysis of compromised terminal
- Security camera footage review
- Authentication system audit
- Access pattern analysis

5 Root Cause Analysis

5.1 Direct Cause

Unauthorized access to GCDB through exploitation of legacy authentication system using unrevoked credentials from a decommissioned terminal.

5.2 Contributing Factors

- Incomplete decommissioning of old terminal in evidence room
- Legacy authentication system running parallel to new zero-trust system
- Improper credential management during system transition

- Insufficient network segmentation
- Inadequate physical security controls in evidence rooms
- Lack of multi-factor authentication on legacy systems

5.3 Root Cause(s)

- **Primary Root Cause:** Failed implementation of decommissioning procedures during infrastructure upgrade
- **Secondary Root Causes:**
  - Incomplete credential audit during system migration
  - Insufficient monitoring of legacy systems
  - Lack of proper access control protocols for evidence rooms
  - Inadequate change management procedures

6 Impact Analysis

6.1 Security Impact

- Unauthorized access to 247 case files
- Exposure of ongoing investigation data
- Potential compromise of confidential informant information
- Access to suspect tracking data

6.2 Operational Impact

- 47 minutes of unauthorized system access
- 1.5 hours of system downtime during investigation
- Delayed access to criminal records for ongoing investigations
- Required revalidation of all system credentials

6.3 Compliance Impact

- Violation of Criminal Justice Information Services (CJIS) security policy
- Mandatory reporting to oversight committee
- Required security audit of all evidence room systems
- Potential policy violations regarding vigilante data access

7 Corrective Actions

Action Item	**Description**	**Owner**	**Due Date**
Legacy Shutdown	Complete removal of legacy authentication system	Dick Grayson	11/30/24
Access Review	Comprehensive review of all system access	Barbara Gordon	12/15/24
MFA Implementation	Deploy MFA across all access points	Timothy Drake	12/01/24
Network Segmentation	Implement enhanced network isolation	Lucius Fox	12/30/24

8 Preventive Actions

Action Item	**Description**	**Owner**	**Due Date**
Security Protocol	Establish formal vigilante access procedures	Commissioner Gordon	12/01/24
Audit Schedule	Implement quarterly security audits	Barbara Gordon	12/15/24
Training Program	Security awareness training for all personnel	Timothy Drake	12/30/24
Access Control	Enhanced physical security measures	Dick Grayson	01/15/25

9 Lessons Learned

- Complete decommissioning procedures must be verified
- Legacy systems pose significant security risks
- Physical security is as critical as digital security
- Formal protocols needed for vigilante cooperation
- Regular security audits must include evidence room systems
- Better coordination needed between physical and IT security teams

10 References

Document ID	**Description**
SEC-2024-113	Security Incident Log
FOR-2024-089	Forensic Analysis Report
LOG-5528-A	System Access Logs
CAM-B13-114	Evidence Room Security Footage

A Appendix A: Technical Analysis

Detailed technical analysis of the breach, including log excerpts and forensic findings.

B Appendix B: Security Recommendations

Comprehensive security enhancement recommendations from Wayne Enterprises.

C Appendix C: Compliance Impact

Detailed CJIS compliance impact analysis and remediation steps.