Incident Investigation

Investigation and Report Done by

Brayden Mitchell

Cloud Services

Table of Contents

Executive Summary

Incident Nature and Scope

A breach has been confirmed affecting Cloud Services on July 6, 2024. Log evidence shows a multiphase attack which originated from a single IP address: 192.168.10.15. Over the course of about 2 hours, the attacker conducted reconnaissance, attempted brute-force logins across several user accounts. The attacker eventually gained administrative access to the system which allowed him to create a new super user and delete system files and the old admin user.

Critical Business Impacts

The confirmed compromise of an admin user presents several risks to Cloud Services. The following impacts are the most critical and should relay the importance of a timely recovery.

1. Potential Exposure of Sensitive Data
    a. As an admin user the attacker had the ability to see, use, and copy confidential data including other user credentials, system configurations, and business and customer records. Not all that was taken can be known because of the deleted logs.
2. Loss of Log integrity and Forensic Visibility
    a. The attacker deleted system logs leading to the concealment of malicious activity. This impacts our ability to perform a complete reconstruction of the system.
3. Elevated Regulatory and Compliance Risk
    a. Mandatory reporting requirements based on the data stolen may have to be implemented and failure to do so could lead to fines or compliance penalties.
4. Operation and Financial Disruption

    a. The reconstruction and investigation will require significant time and recourse which will reduce system availability and increase operational costs as all hands are on deck.

5. Reputational Damage and Loss of Trust
    a. Customer confidence in Cloud Services security posture could be undermined.
6. Risk of Repeat
    a. Due to the amount of time the attacker had he may have created additional backdoors or footholds to enter the system that at this point remain undiscovered. This leaves a vulnerability to exploit for this attacker and any other attacker that notices the openings. Until the systems are fully audited and rebuilt, CloudServices faces the possibility of further compromise.

Most Important Recommendations

Recommendations include immediate system isolation, secure credential resets, SIEM-based monitoring, implementing MFA and adopting security frameworks.

Required Decisions or Approvals

The following decisions must be made by Cloud Services leadership to ensure a timely response and remediation of the confirmed breach.

1. Approve System Isolation
2. Approve Organization Wide Credentials reset
3. Approve the Implementation of MFA
4. Approve Security Program Enhancements

Incident Overview

When and How the Incident was Detected

The incident was first detected at 1:30 on July 6th. The attacker was scanning the network searching for open ports in the system. This was identified on one of the logs. Soon after the brute force attempts began which confirmed an attack.

Systems and Data Potentially Affected

Anything on our system can be at risk. The attacker gained admin access. The data affected could include system log files, cron configuration, and administrative command history.

No logs indicate access to customer, financial, or application data; however due to the attacker gaining administrative privileges, the full scope of data exposure cannot be exclusively determined based on what is shown in the remaining logs.

Initial Response Actions Taken

Once the spike in failed login attempts and correlated scan activity was observed, the following initial steps were taken:

1. Review of authentication logs to determine whether the attacker successfully authenticated
2. Correlation of alerts.log with auth.log to verify whether the same IP (192.168.10.15) was involved in both reconnaissance and login attempts.
3. Inspection of audit logs to assess post-compromise activity. This revealed:
    - Attempts to modify the admin user’s crontab

- Deletion of log files and possibly user command history

  These actions validated the suspicion of a successful breach and triggered deeper forensic review.

Investigation Methodology

1. Log Correlation:
   - Systematically reviewed auth.log for authentication quirks
   - Pulled out patterns of failed logins (744 failures from the same IP)
   - Identified the exact timestamp of successful compromise
2. Alert Analysis:
   - Analyzed alerts.log for reconnaissance events
   - Confirmed scans at 13:49:11 and 14:28:32 targeting MySQL and SSH services
   - Mapped attack activity to MITRE ATT&CK techniques
3. Audit Log Forensics:
   - Located entries showing crontab modification attempts
   - Identified file deletion events indicating defense evasion
   - Assessed whether persistence mechanisms were successfully added
4. Timeline Reconstruction:

   All events were arranged chronologically to understand attacker progression from reconnaissance → brute force → successful login → post-compromise activity.
5. Impact Scoping:
   - Determined likely affected systems
   - Identified compromised credentials
   - Evaluated integrity of system logs and scheduled tasks

This methodology ensured that all findings were supported by validated evidence directly from the logs.

Timeline of Key Investigative Activities

To see the complete timeline find the timeline visual attached to this report. This visual identifies all of the key steps the attacker took and what the attacker did over the time he was in the system. This timeline below identifies the investigative activities.

1. Initial MySQL service scan detected from 192.168.10.15 (alerts.log).
2. Second scan targeting SSH services detected from the same IP.
3. First failed password attempt recorded in auth.log.
4. Total of 744 failed login attempts across multiple user accounts.
5. Successful login as admin from 192.168.10.15.
6. Attacker attempts to modify admin's crontab (audit.log).
7. Attacker executes file deletions, including system log files (audit.log).
8. Final failed login attempt recorded; scripted brute-force attempts continue even after the attacker already has access.
9. Logs reviewed, abnormalities validated, and activity mapped to MITRE ATT&CK techniques.

Technical Analysis

Evidence of Compromise

Multiple indicators across the authentication, alerting, and audit logs confirm that the system experienced a successful compromise on July 6, 2024.

Key evidence includes:

- 744 failed login attempts from the same external IP address (192.168.10.15)
- Successful login as the admin user at 15:04:22 from that same IP
- Reconnaissance scans recorded in alerts.log (MySQL scan and SSH scan)
- Crontab modification attempts under the admin account recorded in audit.log
- File deletion activity, including removal of log files and potentially user history
- High-volume, automated brute-force behavior continuing even after a successful compromise

Attack Vectors and Techniques Used

1. Network Reconnaissance
    a. Alerts identify port and service scans targeting MySQL and SSH services.
    b. Trying to identify open services and potential points of entry.
2. Brute-Force Credential Attacks
    a. 744 consecutive failed login attempts from 192.168.10.15.
    b. Attacker cycled through numerous usernames to find a valid credential.
3. Valid Account Abuse (Successful Login)
    a. The attacker logged in as admin.
    b. Indicates brute-force success rather than vulnerability exploitation.

4. Persistence Attempts
    a. Audit logs show unauthorized attempts to modify admin’s crontab, suggesting the attacker attempted to schedule recurring execution of malicious commands.
5. Defense Evasion
    a. File deletions recorded in audit.log show removal of logs and possible user history.
    b. This indicates the attacker attempted to cover their tracks.

Systems and Data Confirmed to be Affected

The following system components and data were directly affected:

- SSH authentication subsystem
    - This means the attacker didn’t “break in” by force, they logged in as if they were a legitimate administrator, giving them high-level control.
    - Administrative credentials were compromised.
        - This is one of the most serious forms of compromise because it gives attackers broad access to systems and data.
- Cron scheduling subsystem
    - The attacker tried to modify the system’s automated task scheduler, the part of the server that runs jobs on a timer.
        - Changing scheduled tasks is a common way for attackers to make sure they can get back in later, even if their initial access is removed.
    - Attacker attempted to alter scheduled tasks for persistence.

        - This indicates the attacker intended long-term access, not just a one-time intrusion.

- System log files
    - Log files track every login, error and security event
    - Deletion of log files
        - The attacker tried to erase or hide their tracks by deleting security logs.
- Administrative account environment
    - This refers to the personal settings, history files, and environment of a high-level administrator's account.
        - Accessing the bash history for the admin would allow us to see what the attacker performed while on the system.
    - removal or alteration of bash history
        - Does not allow us to identify what the attacker did completely while on the system, the attacker was covering their tracks

Attacker Activities Observed

1. Persistence Attempts via Cron
    a. The audit log records lines confirming crontab edits, indicating the attacker attempted to create or modify scheduled jobs.
    b. This is a common persistence technique used to ensure code executes even if the system reboots or the session ends.
2. Log and Evidence Deletion
    a. Audit logs show execution of rm commands targeting log files.
        i. Rm stands for remove or delete

   b. The attacker was trying to hide invalid login attempts

3. Continued Brute-Force Attempts
   a. Even after the successful login, the brute-force script continued making failed login attempts
   b. This suggests automated tooling rather than manual interaction.
4. Privilege Use
   a. The attacker operated directly under the admin account.
   b. No evidence of privilege escalation beyond this was found, because admin was already a high-privilege account.

MITRE ATT&CK Mapping of Techniques

Stage	**Technique**	**Evidence**
Recconnaissance	Network Service Discovery	2 Alerts
Initial Access	Brute Force	744 failed login attempts
Initial Access	Valid Accounts	Successful admin login
Execution	Command and Scripting Interpreter	Postlogin shell actions
Persistence	Scheduled Task/Job	Crontab modifications in audit.log
Defense Evasion	Indicator Removal	File deletions recorded by audit.log
Credential Access	Password Guessing	Thousands of brute-force attempts

Extent of Potential Data Exposure or Damage

The attacker gained full access to the admin account, which significantly increases the potential scope of impact. Potential exposure or damage include:

- Full visibility into all system files accessible to admin
    - This may include configuration files, user directories, SSH keys, and logs.
- Alteration or deletion of system logs, reducing the ability to reconstruct the incident accurately.
- Potential exposure of sensitive internal data
    - While no exfiltration was observed in logs, the absence of logs due to deletion makes full verification impossible.
- Manipulation of cron jobs, which could have enabled long-term persistence, scheduled malware execution, or automated data removal.
- Integrity loss
    - Tampering with system files, logs, or configurations cannot be ruled out.

Given the administrative level of access, the risk is considered high, even if the confirmed scope of damage is primarily related to log deletion and attempted persistence.

Business Impact Assessment

Operational Impacts (system downtime, business disruption)

The successful unauthorized login to the admin account along with the combined log deletion and attempted persistence mechanisms requires an immediate isolation of the affected system, emergency incident response and interruption of administrative workflows. The security team and IT team's resources will be diverted to emergency response and administrative work that needs the system to be completed will be halted.

Data Impacts (confidentiality, integrity, availability)

Since the hacker had admin access it should be assumed that all data could be potentially exposed. The attacker could have viewed system logs, password files and SSH keys. We know that the attacker attempted to modify user cron jobs which may have altered the systems behavior. Malicious cron jobs could have enabled dangerous actions to the integrity of the system. The deleted log files could impair the system functionality.

Financial Impacts (direct costs, revenue loss, recovery expenses)

Direct Costs

- Incident response labor
- Overtime or reallocation of IT staff
- Potential external forensic consultant fees
- System rebuilding or reconfiguration costs

Indirect Costs

- Lost productivity while systems are investigated or taken offline
- Delayed projects or stalled business operations

Potential Revenue Loss

- Customer services depend on the compromised system therefore, downtime or degraded performance can directly affect revenue streams.

Long-Term Costs

- Investments in additional security tools, monitoring systems, and training
- Increased insurance premiums following an incident

These costs will add up to about $190,000. This number was calculated by using AI using the information on our company, including the number of employees, revenue, and number of customers.

Compliance and Regulatory considerations

Because Cloud Services hosts healthcare, financial, and federal contractor data, the risk of required reporting is extremely high. Even if no confirmed exfiltration occurred, the admin-level access + log deletion would likely trigger notification requirements. These fees and fines could be relatively low at $90,000 but could reach up to over $1 million because the amount is highly dependent on what the compliance organizations determine to be harmful to the customers. This number was also calculated using AI.

Reputational and Customer Trust Implications

Reputational costs are where our company can take a huge hit. Cloud providers in regulated industries lose 3-7% of annual revenue after a breach.(AI) With our revenue at $45 million per year estimated losses fall between $2-4 million.

Total for all costs that will be incurred by Cloud Services is estimated to be $3.8 million. This is 8.5% of Cloud Services Annual Revenue. Again, these numbers were calculated using AI based on our companies demographics and statistics.

Security Recommendations

Immediate Containment and Recovery Actions

Immediate system isolation is an immediate action along with a full credential reset, a rebuild of the compromised system, a preservation process of all log files, a system block on the attacker IP address, an audit of all cron jobs as we know the attacker attempted to modify the cron jobs and re-enabling the system logging settings.

Short and Long-Term Security Improvements

Short-Term

1. Enforce Multi-Factor Authentication on all accounts.
2. Implement an account lockout policy (lock account after 5 failed attempts).
3. Disable password-based SSH login and enforce key-based authentication.
4. Conduct a complete vulnerability scan across the entire system

Long-Term

1. Implement a full SIEM solution (Splunk) for centralized log relations
2. Segment the network to isolate administrative, application, and database systems.
3. Develop and practice a formal Incident Response Plan (IRP) with annual exercises.
4. Conduct penetration testing at least annually, with additional tests after major system changes.
5. Adopt a formal security framework, such as NIST Cybersecurity Framework (CSF)
6. Invest in staff cybersecurity training, especially for IT admins.

Prioritized Implementation Roadmap

Immediate Actions 24-48 Hours

- System isolation and rebuild
- Credential resets
- Multi Factor Authentication
- Firewall blocks for attacker IP
- Restore full logging capabilities

Reason: These steps halt active compromise and restore system trust.

Short-Term Actions 1-4 Weeks

- Implement lockout policies
- Conduct vulnerability scans
- Improve cron, log, and file integrity monitoring
- Begin SIEM deployment planning

Reason: Reduces risk of repeat incidents and improves detection capabilities.

Medium-Term Actions 1-3 Months

- Complete SIEM rollout
- Establish network segmentation
- Conduct penetration testing
- Adopt a security framework (NIST CSF)

Long-Term Actions 3-12 Months

- Conduct Annual penetration testing

- Expand the recovery system so that systems can be restored quickly if another attack happens

Resource Requirements and Constraints

Requirements will include staff positions and technology. Security Analysts will be needed for SIEM configuration. System admins will be needed to make decisions for the hardening and rebuilding of our system. We will need SIEM licensing and storage, secure log storage system software and multi factor authentication management tools.

Expected Outcomes

With the following recommendations implemented, Cloud Services should expect several improvements. Brute-force vulnerabilities will be eliminated because of multi factor authentication and lockout policies. Malicious activity will be detected faster due to SIEM integration. Improved log monitoring will prevent persistence mechanisms that this attacker was able to take advantage of while in our system.