Cymbal

Security Incident Report

Table of contents

Incident Report: Data Breach at Cymbal Retail

Date of Report: July 23, 2025

Executive summary:

On July 23, 2025, Cymbal Retail experienced a significant data breach impacting its cloud environment. The incident was a result of several critical vulnerabilities across Compute Engine virtual machines (VMs), Cloud Storage buckets, and firewall configurations. A malicious actor exploited these vulnerabilities, leading to unauthorized access and potential exposure of sensitive data. Specifically, the compromised Compute Engine VM (cc-app-01) had a public IP address, disabled secure boot, and was utilizing a default service account with full API access, making it a prime target.

Furthermore, the Cloud Storage bucket was publicly accessible due to a public bucket ACL and disabled uniform bucket-level access, allowing unauthorized access to stored objects. Compounding these issues, the firewall rules were overly permissive, with open SSH and RDP ports, and logging was disabled for critical rules, hindering visibility into network traffic. The security team at Cymbal Retail has successfully mitigated the impact of this breach, contained the threat, eradicated the vulnerabilities, and initiated recovery procedures to restore the affected systems to a secure state. This report details the incident, the response actions taken, and recommendations for strengthening Cymbal Retail's cloud security posture against future threats.

Investigation:

A comprehensive investigation was conducted to determine the nature and extent of the compromise. The following findings were identified:

1. **Malware infection**: Forensic analysis confirmed the presence of malware on the compromised VM. The specific type and variant of the malware were identified through in-depth analysis, providing insights into the attacker's techniques and potential motivations.

2. **Unauthorized access**: Evidence revealed that the attacker gained unauthorized access to the compromised VM by exploiting open RDP and SSH services. The access logs and network traffic analysis provided crucial insights into the attacker's entry point and their subsequent activities.

3. **Privilege escalation**: The forensic examination indicated that the attacker leveraged the compromised VM to escalate privileges and gain access to sensitive systems and resources. Through the exploitation of user and service account credentials, the attacker was able to move laterally within the network and target additional services; in particular gaining unauthorized access to BigQuery.

4. **Data exfiltration**: The forensic analysis confirmed the exfiltration of credit card information, including card numbers, user names, and associated locations. The attacker utilized a storage bucket with public internet access to initiate and facilitate the exfiltration, exporting the compromised data for later remote retrieval.

The findings provide valuable insights into the attack, enabling the incident response team to understand the attack vector, the attacker's actions, and the compromised data. These findings will serve as crucial evidence for further investigations, remediation efforts, and future cybersecurity enhancements.

Response and Remediation:

Cymbal Retail's security team executed a multi-faceted incident response to contain, eradicate, and recover from the data breach.

Containment and Eradication Measures:

1. The vulnerable Compute Engine VM, cc-app-01, was immediately shut down by navigating to Compute Engine > VM instances and stopping it.
2. A new, secure VM named cc-app-02 was created from a snapshot and configured with appropriate settings, addressing vulnerabilities such as public IP address, disabled secure boot, and the use of a default service account with full API access.
3. The compromised cc-app-01 VM was subsequently deleted by selecting it on the VM Instances page and clicking "Delete".
4. Public access to the Cloud Storage bucket was remediated by switching the bucket's access control to uniform and removing permissions for the allUsers principals. This involved navigating to Cloud Storage > Buckets, selecting the vulnerable bucket, going to its Permissions, selecting "Switch to uniform," ensuring "Add project role ACLs to the bucket IAM policy" was selected, and then removing access for allUsers.
5. Overly permissive default firewall rules, specifically default-allow-icmp, default-allow-rdp, and default-allow-ssh, were identified and deleted.
6. A new firewall rule named limit-ports was created to restrict SSH (TCP port 22) access. This rule limits access to only authorized IP addresses from the source network 35.235.240.0/20 for Compute Engine VM instances with the target tag cc.

Recovery Measures:

1. The creation of the cc-app-02 VM from a known good snapshot ensured the restoration of application functionality from a secure and uncompromised state.

2. By enabling uniform bucket-level access for the Cloud Storage bucket and implementing the restrictive limit-ports firewall rule, the configurations of critical cloud resources were secured to prevent recurrence of similar vulnerabilities.
3. Logging was enabled for the newly created limit-ports firewall rule and the existing default-allow-internal firewall rule. This was achieved by editing each rule's details and selecting "On" in the Logs section. This action significantly enhanced visibility and auditing capabilities for network access

Recommendations:

Based on the findings and remediation efforts, the following recommendations are crucial for improving Cymbal Retail's cloud security posture:

1. **Implement Principle of Least Privilege for Service Accounts:** Review and strictly enforce the principle of least privilege for all service accounts within the cloud environment. The use of default service accounts with full API access significantly contributed to the breach. Future configurations should only grant the minimum necessary permissions required for an application or service to function, reducing the potential impact of a compromise.
2. **Automate Security Configuration Audits and Enforcement:** Implement automated tools and processes to regularly audit cloud resource configurations against predefined security benchmarks and policies. This includes continuous monitoring for publicly exposed resources, misconfigured access controls on storage buckets, and overly permissive firewall rules. Automated enforcement can proactively address deviations from security best practices before they lead to incidents.
3. **Strengthen Network Segmentation and Microsegmentation:** Enhance network segmentation beyond basic firewall rules. Consider implementing microsegmentation strategies to isolate critical applications and data within their own network segments. This limits lateral movement for attackers, even if a perimeter defense is breached, significantly containing the scope and impact of future security incidents.

4. **Mandate and Monitor Comprehensive Logging and Alerting:** While logging was enabled post-incident, a robust, enterprise-wide logging strategy with real-time alerting is essential. Ensure that flow logs for all VPC subnets are enabled and that alerts are configured for suspicious activities, unauthorized access attempts, and changes to critical security configurations. This proactive monitoring is vital for early detection and rapid response to emerging threats.