NETSPI

Threat Model

Project: Groupon Production Environment

Groupon

March 11th, 2022

NETSPI

Contents

Chapter 1 | Executive Summary

Between the dates of January 18th and March 11th, NetSPI performed a threat model of Groupon's production environment. Groupon production is undergoing a major cloud migration to AWS between Q1 and Q2 of 2022. The goal of this assessment was to identify potential areas of security risk within the Groupon architecture and security practices.

Finding Summary

During this engagement, NetSPI identified several positive aspects of Groupon's architecture. This list is not exhaustive, but identifies a few specific design elements in place that increase the overall security of Groupon production, making certain attacks more difficult for a would-be attacker to execute:

- The use of mutual TLS (mTLS) sidecars for all non-public containerized services.
- An internal PKI with offline root certificates.
- The use of Envoy-based Hybrid Boundary solution for orchestrating container-based service authorization.

NetSPI identified 7 security risks:

- 0 Critical-Severity
- 3 High-Severity
- 2 Medium-Severity
- 2 Low-Severity

Some of the key security risks include:

- Lack of application security and business continuity programs.
- The use of GitHub Enterprise for managing secrets.
- The use of client tokens to affect a long-lived session scheme for client devices.

Recommendation Summary

NetSPI recommends Groupon begin the remediation of identified risks using the prioritized approach below:

- Develop a centralized application security program to handle application-level security activities both in and out of the SDLC, such as static analysis security testing, software composition analysis, a security champions program, application-security incident response, patch and update assistance for third party commercial and open-source libraries, frameworks, and middleware, and security architecture functions.
- Develop secrets management solutions for AWS, GCP, and on-premise management of application secrets which supports access auditing, secrets rotation, and compliance for complexity standards.
- Replace client tokens with JWTs in adherence with best practices for securing consumer-facing / retail services.

Chapter 2 | Project Summary

NetSPI performed an analysis of Groupon production to identify vulnerabilities, determine the level of risk they present to Groupon, and provide actionable recommendations to reduce this risk. NetSPI compiled this report to provide Groupon with detailed information on each vulnerability discovered within the application, including potential business impacts and specific remediation instructions.

2.1 Project Overview

NetSPI's primary goal within this project was to provide Groupon with an understanding of the current level of security in its production environment.

NetSPI completed the following objectives to accomplish this goal:

- Interview key system stakeholders to understand business context, implementation details, and system risks
- Review available documentation to support deeper understanding of the application
- Construct a threat model diagram to facilitate analysis of attack scenarios and system vulnerabilities and risks
- Identify application-based threats to and vulnerabilities in the application
- Compare Groupon's current security measures with industry best practices
- Provide recommendations that Groupon can implement to mitigate threats and vulnerabilities and meet industry best practices

2.2 Scope and Constraints

The following components were in scope for this threat model:

- The production Groupon environment

2.3 Summary of Findings

NetSPI's assessment of the service revealed the following vulnerabilities:

ISSUE NAME	SEVERITY
Credentials Stored in GitHub Repositories	High
Lack of Application Security Program	High
Lack of Business Continuity or Disaster Recovery Plan	High
Lack of Supply Chain Controls	Medium
Improper Sessioning	Medium
Developer Access to Production Console	Low
Backup System Design Not Resilient to Regional Outage	Low

TABLE 1: FINDINGS SUMMARY

Chapter 3 | Threat Model

The analysis performed in this assessment was guided by a threat model diagram that was constructed from existing system and network documentation and information obtained from stakeholder interviews. The threat model diagram is composed of a system component diagram, assets, security controls, and threat actors. This threat model diagram is subsequently analyzed to create possible attack scenarios.

3.1 System Description

The production Groupon environment uses Services Oriented Architecture principles to compose some 700+ services into a two-sided marketplace connecting 24 million customers to local merchants across the globe.

Groupon has implemented many cloud native security controls in its AWS and GCP environments. Services are containerized with a sidecar pattern implementing mutual TLS which not only protects the confidentiality and integrity of data in transit between services, but also authenticates services to one another. These services are orchestrated with Hybrid Boundary which controls service-to-service authorization. Groupon manages server keys with in-house PKI featuring an offline root certificate. Secrets are managed via Github enterprise repos.

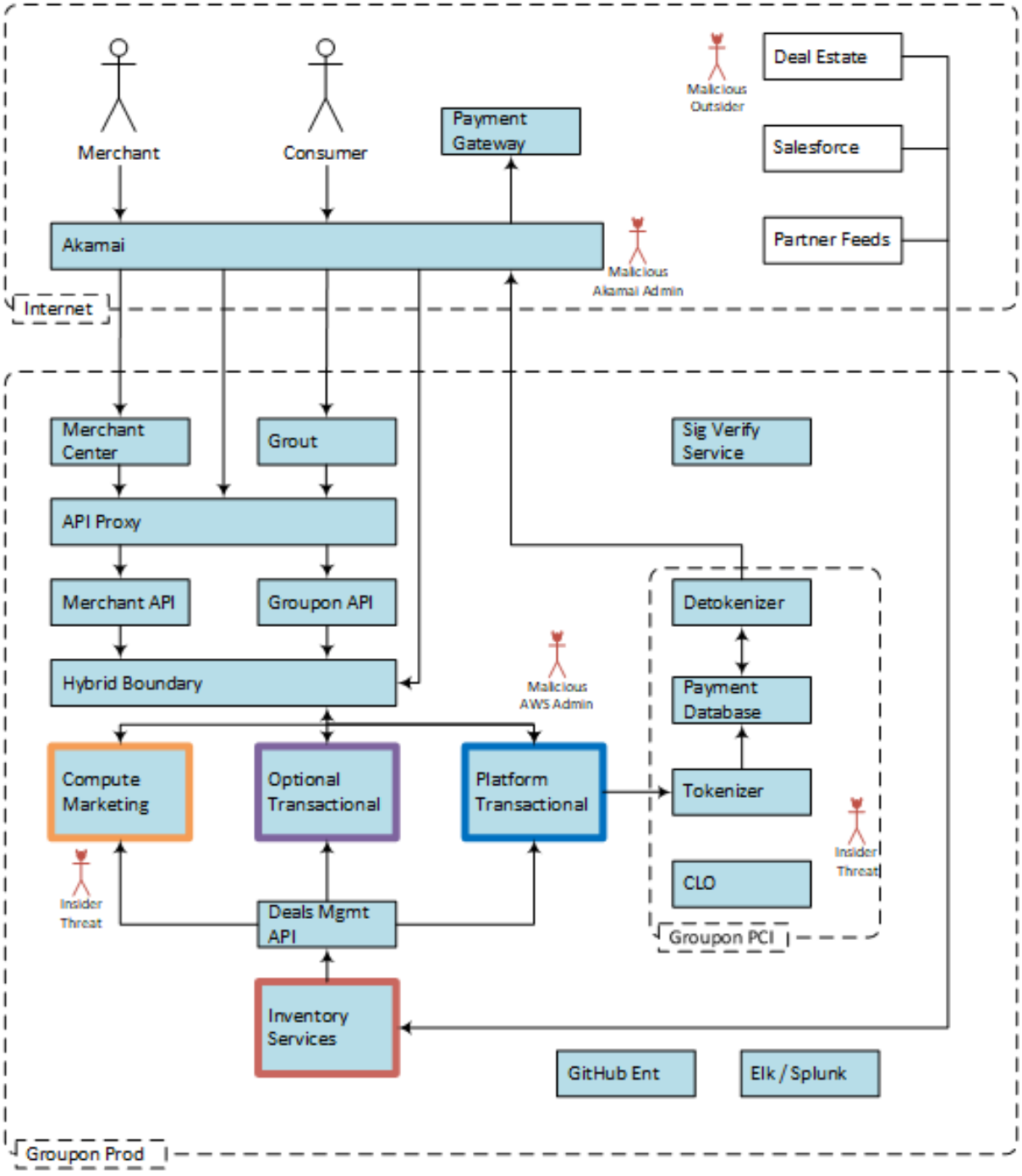
Groupon uses data science extensively, from improving user experience by identifying and catering, to user preferences, to fraud detection.

Edge security services are largely provided by an extensive Akamai implementation. API Proxy mediates access to front-end services. Partners communicate to Groupon APIs with signed partner tokens.

Groupon maintains a mobile first user experience for customers—75% of customer purchases take place from the mobile app—while the merchant UI is largely desktop browser driven. Groupon uses self-describing security tokens to identify client devices.

In the immediate future Groupon will move a large amount of its on-premise services to AWS, with data persistence services being hosted in GCP. Groupon also has projects to refactor its security tokens as JWTs and to refactor its credential repos using AWS Secrets Manager.

3.2 **Component Diagram**



3.3 **Assets**

In this analysis, an asset is anything that warrants protection. Threat actors are typically motivated by accessing or compromising assets of a system.

Consumer and merchant data comprise the lion's share of data processed by Groupon and are central to producing revenue. Cardholder data and cached payment data have a particular relationship: cached payment data is cardholder data in an encrypted or tokenized form. As such the confidentiality requirements are lower for cached payment data—that is the value proposition that tokenization offers us. GitHub secrets are those application secrets currently stored in GitHub enterprise repos. In the future they may be named something else. Subscription offers are coupon-valued individually but attackers have a tendency to go after them en masse.

The below table lists each asset, the title used to denote that asset where it appears on the threat model diagram, a brief description, and a High-to-Low rating of the importance of each asset's Confidentiality, Integrity, and Availability, (C, I, and A, respectively):

Asset Title	Asset Name	Description	C	I	A
ConData	Consumer Data	Customer Email IDs, phone number and passwords.	High	High	Medium
MerData	Merchant Data	Merchant email IDs and passwords.	High	High	Medium
CHData	Cardholder Data	Raw (detokenized) payment data.	High	High	Low
GHSec	GitHub Secrets	Production secrets such as API keys and system credentials are stored in private enterprise GitHub repos. During deploy, secrets are injected into the containers as environment variables.	High	Low	High
TknCCs	Cached Payment Data	Encrypted and tokenized credit card data cached for future purchases.	Low	High	Low
Offers	Subscription Offers	Limited coupons offered in Groupon - attackers will scoop up the coupons and resell them.	Low	Low	High

3.4 **Security Controls**

Security Controls are in place to protect the system and its assets from abuse. Security Controls can take the form of system configuration, features, third party systems, or processes.

Groupon relies on Akamai for a considerable amount of perimeter defense. Internally, Groupon uses a combination of mutual TLS, envoy-based Hybrid Boundary, and a private public key infrastructure featuring offline root certificates to provide internal defense-in-depth. Some cloud-native technologies such as AWS CloudTrail are used.

The below table lists each control, the title used to denote where it appears in the threat model diagram, and a yes/no value as to whether this control defends the confidentiality, integrity, or availability (C, I, and A, respectively) of the asset it protects:

Control Title	Control Name	Description	C	I	A
Private PKI	Private PKI	Five intermediate CAs are trusted across Groupon and Akamai with offline root certificates.	Y	Y	Y
Akamai	Akamai	AppSec filtering, coarse-grained geo-blocking, TOR exit node blocking, L7 DDOS protection, rate limiting, out-of-date user-agent blocking, custom CC-match blocking, etc.	Y	Y	Y
RBAC	Role Based Access Control	Conveyor (Kubernetes) team, database, platform (AWS/GCP), and other teams have access to different things based on role assigned.	Y	Y	Y
AWS Config	AWS Config	Config continuously monitors and records AWS resource configurations and allows owners to automate the evaluation of recorded configurations against desired configurations.	Y	Y	Y
AWS CloudTrail	AWS Cloud Trail	CloudTrail records actions taken by a user, role, or an AWS service.	Y	Y	N
Hybrid Boundary	Hybrid Boundary (Envoy)	AWS proxy layer which routes between Groupon services. Validates traffic is coming from trusted sources (Akamai, on-prem), and enforces MTLS. No services talk directly to each other - they go through Hybrid Boundary.	Y	Y	Y
MTLS Sidecar	Mutual TLS Sidecar	Used for deploying services in EKS and securing service to service communication.	Y	Y	Y
PCI	PCI Controls	All Groupon does to adhere to the PCIDSS.	Y	Y	N
Logs	Logs	Security-relevant events logged in Splunk and Elk.	N	Y	Y
CD Crypto	CachedPaymentData	Tokenized credit card information. When paired with the internal detokenizer and the appropriate key, a valid CC is returned.	Y	Y	N
CustAuth	Customer Authentication	Consumer and Merchant account authentication. Separate from RBAC.	Y	Y	N

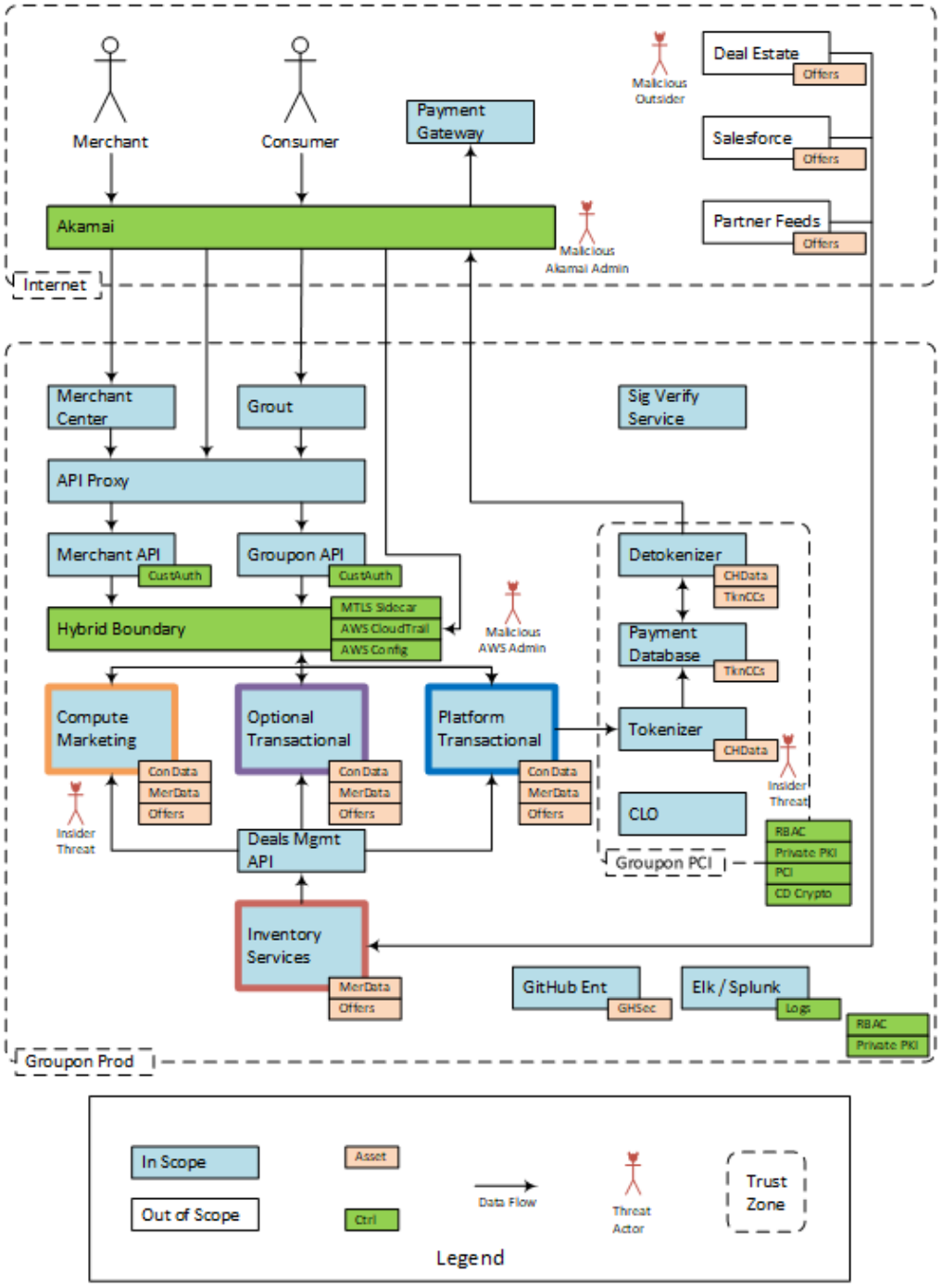
3.5 **Threat Actors**

Threat Actors are typically individuals, events, software, or some other entity that may act against the system, disrupting its behavior and causing it to fail or behave in unexpected ways. The threat actors considered in this model are described below.

THREAT ACTOR	DESCRIPTION
Insider Threat	Any malicious or compromised internal actor including disgruntled users or administrators, compromised workstations, malware uploaded to servers, etc.
Malicious Outsider	Typical malicious internet-based threats, such as hackers, malware campaigns, fraudsters, fraudulent Groupon users, dishonorable merchants, etc.
Malicious AWS Admin	Amazon Web Services-based attackers intent on doing harm or taking advantage of Groupon.
Malicious Akamai Admin	Akamai employees intent on doing harm or taking advantage of Groupon.

3.6 **Threat Model Diagram**

By overlaying the system component diagram above with visual cues indicating the presence of Assets and Controls, by denoting the trust zones identified from boundaries between cohesive infrastructures, and by locating threat actors within those trust zones, it becomes the below threat model diagram:



Chapter 4 | Technical Detail

4.1 Traceability Matrix

The traceability matrix lists all risks - those managed by existing controls, as well as those unmanaged risks discovered during this assessment.

The purpose of this matrix is to aid in making security-relevant architecture decisions. The controls listed in the first column prevent threat actors from using attack patterns listed in the second column from exploiting the attack surfaces, system components, and assets in the third column. The fourth column describes the risk of a successful attack. The fifth column describes how much of that risk is mitigated by the control.

Item	Description
Control	The in-place, technical or administrative control which manages risk down to an acceptable level.
Threat Actor & Attack Pattern	The relevant threat actor that can attack the system and the pattern they might use to exploit a vulnerability.
Attack Surface / System Component & Assets	The place that an attack might happen, and the information assets at risk.
Severity, Impact & Likelihood	Qualitative descriptions of the risk.
Residual Risk	A qualitative measure of risk left unmanaged by the control.

The below traceability matrix lists these risks. Section 4.3 - 4.5 below provides additional details on the unmanaged risk identified during this engagement.

Control	Threat Actor & Attack Pattern	Attack Surface & Assets	Severity (Impact / Likelihood)	Residual Risk
Managed risks. These controls are sufficient from a design perspective to manage the risks listed. Architectural changes should be reviewed to make sure they do not alter the efficacy of these controls.				
Role Based Access Control	Threat Actor: Malicious outsider Attack Pattern: Authorization bypass, privilege escalation	AS: Groupon production, Groupon API, merchant API Assets: Customer data, merchant data	High (High / High)	None
Hybrid Boundary (Envoy)	Threat Actor: Insider threat, malicious AWS admin Attack Pattern: Authorization bypass	AS: Inter-service communication Assets: Customer data, merchant data	High (High / High)	None

Control	Threat Actor & Attack Pattern	Attack Surface & Assets	Severity (Impact / Likelihood)	Residual Risk
Mutual TLS Sidecar	Threat Actor: Insider threat, malicious AWS admin Attack Pattern: Active or passive MITM	AS: Container based services Assets: Customer data, merchant data	High (High / High)	None
PCI Controls	Threat Actor: Insider threat, malicious AWS Admin Attack Pattern: Data exfiltration	AS: Groupon PCI environment Assets: Card data, cached payment data	High (High / High)	None
Signature Verification Service	Threat Actor: Malicious or compromised business partner Attack Pattern: Supply chain attack	AS: Supply layer Assets: Customer data, merchant data	High (High / High)	None
Akamai, Fraud Protection	Threat Actor: Malicious outsider Attack Pattern: Credit card oracle abuse	AS: Groupon API Assets: Corporate image	Medium (Medium / High)	None
AWS Config AWS CloudTrail	Threat Actor: Insider threat, malicious AWS admin Attack Pattern: Data exfiltration, denial of service	AS: Groupon production Assets: All	Low (Medium / Low)	None
Unmanaged risks. These controls are insufficient (or absent) from a design perspective to manage the risks listed, and architectural changes are necessary to fully manage risk.				
None	Threat Actor: N/A Attack Pattern: Disaster	AS: Groupon production Assets: All	High (High / High)	High

Control	Threat Actor & Attack Pattern	Attack Surface & Assets	Severity (Impact / Likelihood)	Residual Risk
None	Threat Actor: Insider threat, malicious AWS admin, compromised application Attack Pattern: data exfiltration, directory traversal	AS: Cloned secrets repo Assets: GitHub secrets	High (High / High)	High
None	Threat Actor: Malicious outsider Attack Pattern: Application level attack	AS: Groupon production, Groupon API Assets: All	High (High / High)	High
None	Threat Actor: Malicious outsider Attack Pattern: Software supply chain compromise	AS: Groupon software dependencies Assets: All	High (High / High)	Medium
Akamai Service Rate Limiting	Threat Actor: Malicious outsider Attack Pattern: Mass account creation	AS: Groupon API Assets: Subscription offers	Medium (Medium / High)	Low
ELK Cluster Splunk	Threat Actor: Insider threat, malicious AWS admin Attack Pattern: Log deletion	AS: All Assets: All	Medium (Medium/Medium)	Low
AWS Config AWS CloudTrail	Threat Actor: Insider threat Attack Pattern: Data exfiltration	AS: Console Assets: All	Low (Medium / Low)	Low

4.2 **Findings Overview**

The detailed findings section contains the analysis and documentation of the vulnerabilities identified within the application. This analysis included:

- Identifying potential vulnerabilities associated with the application
- Assigning appropriate severity rankings to valid vulnerabilities and risks
- Formulating useful action-based recommendations that can improve the security posture of the IT environment

Vulnerabilities are grouped according to severity. Information for each of the vulnerabilities includes the following:

Name: The name of the vulnerability.

Severity: Each of the vulnerabilities has been assigned a severity based on its impact to the system and its associated resources, and the likelihood of a successful exploitation, per NIST SP800-30.

Attack Surface / System Component: The parts of the system affected by this risk.

Risk Details: Comprehensive explanation of the vulnerability that was found, including a high-level summary of how the vulnerability works.

Impact: This describes the potential business impact of the vulnerability, should it be exploited.

Likelihood: This describes the likelihood that the vulnerability will be exploited.

Recommendations: NetSPI's recommended solutions for repairing the vulnerability or mitigating the problem.

4.3 High Severity Findings

4.3.1 Credentials Stored in GitHub Repositories

Severity: High (Impact: High / Likelihood: High)

Attack Surface / System Component

- Enterprise GitHub

Risk Details

Application secrets are stored in Enterprise GitHub repositories. Enterprise GitHub has fine-grained access controls to repositories, which is a good feature to have for a secrets management system. It also has several features which are bad for secrets management, such as decentralization, no built-in encryption, no auditing for who accessed which secrets at what times, and the ability to copy a repository to a thumb drive. An On-prem attacker (either a malicious insider or a compromised account) with unauthorized access to GitHub repositories could exfiltrate application secrets en masse. In addition, Groupon's implementation of service accounts grants broad access to GitHub repositories across multiple teams, functionally bypassing the fine-grained access controls.

Impact

High: A successful attack gives an attacker direct access to Groupon production data and potentially access to Groupon Kubernetes infrastructure and other systems. As the secrets are not checked for complexity requirement and are not rotated frequently, this gives an attacker longer usability window with the acquired credentials.

Likelihood

High: Exfiltration of at least one such repo is reported to already have happened.

Recommendations

Groupon is already evaluating AWS Secrets Manager to store credentials for AWS environment. Something similar must be implemented for on-prem and GCP environments.
To mitigate the risk of storing secrets in GitHub repositories, Groupon should implement secrets management systems which provide below features:

- Tight access controls
- Audit access to credentials
- Check for complexity of secrets
- Secrets rotation

4.3.2 Lack of Application Security Program

Severity: High (Impact: High / Likelihood: High)

Attack Surface / System Component

- Enterprise Delivery Pipeline

Risk Details

Application security activities are largely not performed in the Enterprise Delivery Pipeline. SonarQube is used for static analysis but in very limited scope, looks for code quality and very limited application-level security vulnerabilities. There was no mention of secure coding guidelines, application security dashboards or defect discovery process to evaluate application security risks. We didn't hear about software composition analysis checks in the pipeline. Application security activities aim to identify vulnerabilities in application/services source code and other third-party libraries. These vulnerabilities can allow an attacker to cause harm to Groupon systems. Examples include:

- Modification or exposure of Groupon data
- Arbitrary command execution
- Data exfiltration

Impact

High: Application security programs exist because traditional network capabilities are unable to defend against application attacks.

Likelihood

High: According to the 2021 Verizon DBIR, web application vectors accounted for 90 percent of data breach incidents last year.

Recommendations

NetSPI recommends integrating application security activities like static code analysis and software composition analysis checks into the delivery pipeline. We heard that Groupon is evaluating OWASP Dependency-Checker for software composition analysis. NetSPI recommends SAST/SCA tools which provide below features:

- Regular rules/attack pattern updates
- Active maintenance and support for the product
- Integrates into the enterprise delivery pipeline

4.3.3 Lack of Business Continuity or Disaster Recovery Plan

Severity: High (Impact: High / Likelihood: High)

Attack Surface / System Component

- Groupon production

Risk Details

The business continuity / disaster recovery function (BC/DR) is yet to be rebuilt at Groupon. Without a comprehensive BC/DR program, Groupon is at risk of losing business revenue and merchant/customers as well, especially with availability being key piece for Groupon business operations. Business continuity and disaster recovery plans help an organization be prepared and handle the situation when a disaster or active attack is in progress like Ransomware. Lack of business continuity and disaster recovery can lead to:

- Loss of reputation
- Loss of potential business
- Compliance or SLA violations

Impact

High.

Likelihood

High**.**

Recommendations

NetSPI recommends identification of personnel to own responsibility for all BC/DR activities including incident response, developing, and maintaining BC/DR policies, standards, and runbooks, leading tests and tabletop exercises, etc.

4.4 Medium Severity Findings

4.4.1 Lack of Supply Chain Controls

Severity: Medium (Impact: Medium / Likelihood: Medium)

Attack Surface / System Component

- Groupon software dependencies

Risk Details

Groupon's current supply chain controls are insufficient for preventing the introduction of malicious code into the production environment. Groupon lacks deliberate malicious code detection and has no centralized means of tracking a software bill of materials for its services.

Impact

Medium: A successful attack potentially exposes sensitive user data or credit card information.

Likelihood

Medium: According to the ENISA report *Threat Landscape for Supply Chain Attacks* (https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks), "supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021".

Recommendations

Develop a program to manage near-supply-chain and far-supply-chain risks from both in-house developers, as well as third party developers, and everything in between, for example contract development.

At a minimum, a software supply chain risk program should include considerations for the automatic build-time generation of software bills of materials, which facilitate finding and fixing supply chain vulnerabilities, and a discovery capability for finding malicious code produced by in-house personnel responsible for the development, build, and deployment of software.

4.4.2 **Improper Sessioning**

Severity: Medium (Impact: Medium / Likelihood: Medium)

Attack Surface / System Component

- Security Tokens

Risk Details

Groupon does not maintain authenticated user sessions in accordance with industry best practices. The current security tokens used to identify users are long-lived and are otherwise valid until an authenticated user logs out. In addition, users are not notified of logins from new devices, so a session hijack might go unnoticed for a prolonged period.

Impact

Medium: A successful attack gives an attacker direct access to Groupon user accounts.

Likelihood

Medium: Concerns around security tokens come up frequently even though many consumer-facing sites have long-lived session tokens and few actual problems. That said, the structure of security tokens make it difficult to interoperate, and give every indication of a misuse of cryptographic primitives "under the hood."

Recommendations

Groupon indicated that an effort is underway to replace the existing session tokens with JWTs. NetSPI recommends that this implementation includes:

- Email notification for new device logins.
- Mass session invalidation capabilities in the event of a wide-scale breach.
- Secondary authentication prompts for sensitive functionality.

Use guidance from OWASP on how to implement Java Web Tokens correctly and effectively: https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html

4.5 Low Severity Findings

4.5.1 Developer Access to Production Console

Severity: Low (Impact: Medium / Likelihood: High)

Attack Surface / System Component

- Groupon production

Risk Details

Developers with access to production will be able to access the host console directly and can therefore introduce arbitrary changes to the host outside of the automated deployment pipeline.

Impact

Medium: console access could potentially allow access to sensitive data and a method for exfiltration.

Likelihood

Low: changes to host configurations are logged and alerted on by AWS Config. The Incident Response team would be able to roll back any changes quickly.

Recommendations

The quick way to work down this risk is simply to remove developer access to the production console and forget about it. In so doing, Groupon might be missing out on potential benefits. To the extent that Groupon has benefited in the past from developers having fast access to production should be measured. If additional capabilities are necessary, either for break-glass solution to production problems, improved metrics for product ownership, or statistics for the improvement of performance, formal systems can be created to account for these without the risk of direct developer access to production.

4.5.2 Backup System Design Not Resilient to Regional Outage

Severity: Low (Impact: High / Likelihood: Low)

Attack Surface / System Component

- AWS Backups

Risk Details

The ADM articulating the design considerations for AWS Backups and Restores dictate that AWS backups be performed in the same region but under different accounts.

Several different, competing pressures (called requirements in this document, but they function more like pressures) are documented and several AWS backup solutions are presented. One pressure is that backups be performed to different regions so that if one region goes down, restoration can take place elsewhere. Another is that they be performed to different accounts to avoid the accidental "fat-fingering" causing either loss of backups or possibly the loss of production data if backups are erroneously restored to operational systems, thus stomping data created since the backup was taken. No one backup scheme allows for backup to a different account in a different region.

The document indicates that of the two competing pressures, backup up to different accounts should take precedent over backing up to different regions.

Impact

High: Any extended AWS regional outages can lead to Groupon not being able to recover in another availability zone and will impact business continuity.

Likelihood

Low: The likelihood of an extended AWS regional outage is low. While 17 AWS outages have occurred in the past 11 years, none of them have lasted more than a few days.

Recommendations

Consider the possibility that two backup schemes be utilized. The first would backup locally to a different account. The second would backup that backup to a different region under the same backup account. This should cover both requirements as well as allow for an in-region backup of data which is likely to be restored faster than having to retransmit an out-of-region backup to the down systems.

Appendix A | NetSPI Contact Information

Please contact NetSPI with any questions regarding the findings, analysis, or recommendations contained in this report.

Principal Consultant
Mike Doyle
mike.doyle@netspi.com
678-656-7458

Security Consultant II
Michael Albin
michael.albin@netspi.com
940-704-0302

Security Consultant
Rishabh Jain
rishabh.jain@netspi.com

Project Manager
Brianna Miller
brianna.miller@netspi.com
612-267-6797

Account Manager
Hank Seward
hank.seward@netspi.com
651-571-6211

Revision History

VERSION	DATE	AUTHOR	COMMENTS
0.1	March 8, 2022	Mike Doyle	Document created
0.2	March 9, 2022	Michael Albin	Report QA
1.0	March 10, 2022	Mike Doyle	Report delivery
1.1	March 10, 2022	Michael Albin	Report update based on initial readout

© 2022, NetSPI

This confidential document is produced by NetSPI for the internal use of Groupon. All rights reserved. Duplication, distribution, or modification of this document without prior written permission of NetSPI is prohibited.

All trademarks used in this document are the properties of their respective owners.