Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Fri Oct 11 2024

Executive Summary

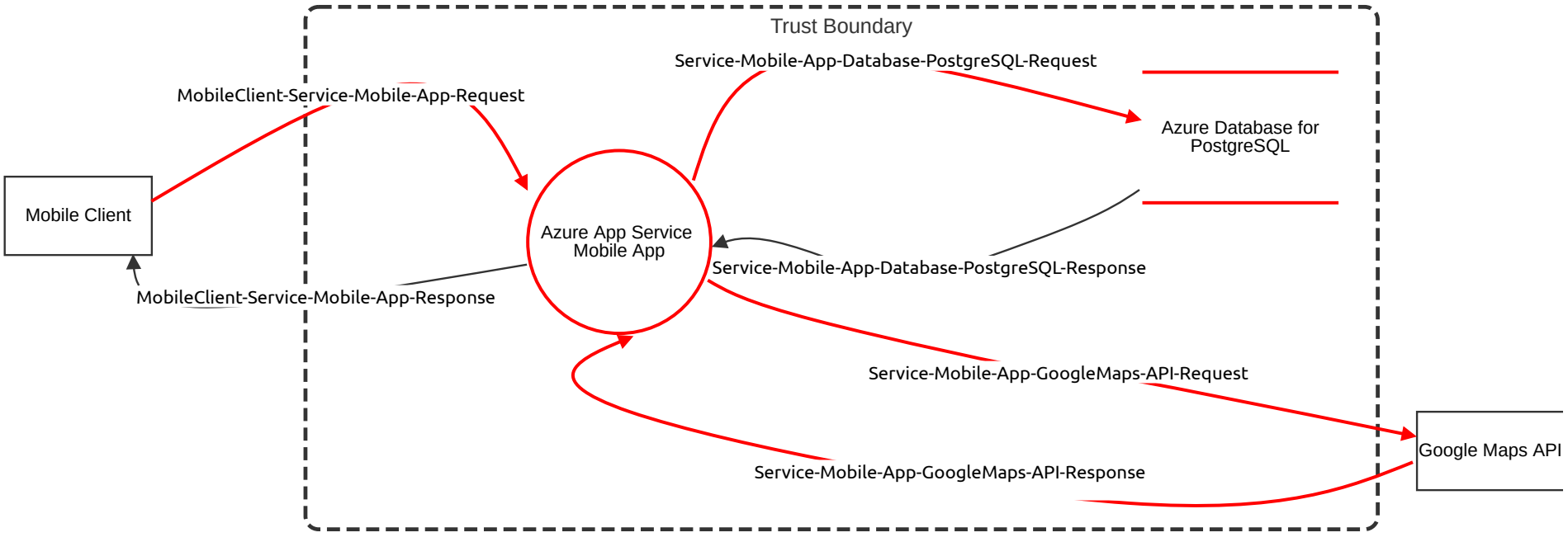
High level system description

Not provided

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	2
Open / Medium Priority	8
Open / Low Priority	0
Open / Unknown Priority	0

Catrip


Trust Boundary
Service-Mobile-App-Database-PostgreSQL-Request
MobileClient-Service-Mobile-App-Request
Azure Database for PostgreSQL
Mobile Client
Azure App Service Mobile App
Service-Mobile-App-Database-PostgreSQL-Response
MobileClient-Service-Mobile-App-Response
Service-Mobile-App-GoogleMaps-API-Request
Google Maps API
Service-Mobile-App-GoogleMaps-API-Response

Catrip

Mobile Client (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Azure Database for PostgreSQL (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	An adversary may read and/or tamper with the data transmitted to Azure Postgres DB due to weak configuration	Tampering	Medium	Open		An adversary may read and/or tamper with the data transmitted to Azure Postgres DB due to weak configuration	Provide remediation for this threat or a reason if status is N/A

Google Maps API (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Azure App Service Mobile App (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	An adversary may gain long term persistent access to related resources through the compromise of an application identity	Elevation of privilege	High	Open		An adversary may gain long term persistent access to related resources through the compromise of an application identity	Provide remediation for this threat or a reason if status is N/A
10	An adversary may perform action(s) on behalf of another user due to lack of controls against cross domain requests	Elevation of privilege	Medium	Open		An adversary may perform action(s) on behalf of another user due to lack of controls against cross domain requests	Provide remediation for this threat or a reason if status is N/A
12	An adversary may perform action(s) on behalf of another user due to lack of controls against cross domain requests	Elevation of privilege	High	Open		An adversary may perform action(s) on behalf of another user due to lack of controls against cross domain requests	Provide remediation for this threat or a reason if status is N/A
13	Attacker can deny a malicious act on an API leading to repudiation issues	Repudiation	Medium	Open		Attacker can deny a malicious act on an API leading to repudiation issues	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	An adversary may spoof Azure App Service Mobile App and gain access to Web API	Spoofing	Medium	Open		If proper authentication is not in place, an adversary can spoof a source process or external entity and gain unauthorized access to the Web Application	Provide remediation for this threat or a reason if status is N/A

MobileClient-Service-Mobile-App-Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

MobileClient-Service-Mobile-App-Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	An adversary can fingerprint an Azure web application or API by leveraging server header information	Information disclosure	Medium	Open		An adversary can fingerprint an Azure web application or API by leveraging server header information	Provide remediation for this threat or a reason if status is N/A

Service-Mobile-App-Database-PostgreSQL-Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	An adversary may block access to the application or API hosted on Azure App Service Mobile App through a denial of service attack	Denial of service	Medium	Open		An adversary may block access to the application or API hosted on Azure App Service Mobile App through a denial of service attack	Provide remediation for this threat or a reason if status is N/A

Service-Mobile-App-Database-PostgreSQL-Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Service-Mobile-App-GoogleMaps-API-Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	An adversary can gain access to sensitive data by performing SQL injection through Web API	Tampering	Medium	Open		SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	Provide remediation for this threat or a reason if status is N/A

Service-Mobile-App-GoogleMaps-API-Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	An adversary may block access to the application or API hosted on Azure App Service Mobile App through a denial of service attack	Denial of service	Medium	Open		An adversary may block access to the application or API hosted on Azure App Service Mobile App through a denial of service attack	Provide remediation for this threat or a reason if status is N/A