RIGGS EXAMPLE MOBILE APP
RISK ASSESSMENT REPORT

File Name	com.riggsexamplemobileapp.apk
SHA-1	CC36BC13EC0A1C52F387B0BF5C9027C2FC3DF8E1
Date/Time of Analysis	1st July 2023 – approx 20:00 PM (GMT)
Report Author	Jacob Riggs (Security Researcher)
Business Unit Requesting	Finance and Procurement
Risk Owner	Assistant Director of Finance
Business Justification	The proposed application offers an innovative solution for simplifying financial operations and management. It provides our employees with instant access to real-time financial data, robust analysis tools, and streamlined processes for financial planning, invoicing, and reporting. These capabilities will significantly increase the efficiency and accuracy of our financial management processes, fostering better informed decision making across all levels of the organisation. Despite our current financial systems, there remains a significant gap in the real-time access to financial data and the ability to perform on-the-go financial tasks. The proposed application fills this gap by providing a mobile platform for finance operations, enabling staff to access and manage financial information anytime, anywhere. This flexibility is particularly essential for our remote and on-field employees, and during travel or off-site meetings.

Application Permissions	**Risk Level**
The application requests several permissions that appear to be unnecessary for its stated functions. These include access to contacts, call logs, and messages. The app's request for such personal and sensitive data without clear necessity raises major privacy concerns. This could potentially lead to unauthorised	**HIGH**

data access or leakage if misused, either intentionally or unintentionally. Given the highly personal nature of these data types, this risk is currently evaluated as High.	
Recommendation	
The business should engage with the app's developer to understand the necessity of the broad permissions requested by the app. If no satisfactory rationale is provided, the business should request a revision of the permissions to restrict access only to essential data and functionalities.	

Network Activity Analysis	**Risk Level**
During the analysis, it was noted that the application communicates with several servers, some of which have been associated with serious data breaches in the past. The app also sends potentially sensitive user data to these servers. Furthermore, some connections were observed to use unencrypted HTTP instead of HTTPS, which could expose sensitive user data to potential interception. Given the severity of past breaches associated with these servers and the insecure transmission methods used, the risk level associated with network activity is evaluated as High.	**HIGH**
Recommendation	
Request the developer to shift all data transmission to secure, encrypted connections, ideally HTTPS. Also, demand clarity on the nature and necessity of the communication with servers associated with past breaches.	

Secure Data Transmission	**Risk Level**
The application uses Transport Layer Security (TLS) for all data transmission, ensuring data transferred is encrypted and protected from interception.	**ACCEPTABLE**

Application Components	**Risk Level**
The app was built using modern, secure coding techniques and does not appear to use any deprecated or vulnerable libraries.	**LOW**

However, the use of some third-party frameworks not reviewed in this assessment may require additional analysis.	

App Store Records	Risk Level
The developer has a good reputation, regular update frequency, and the app has mostly positive reviews. However, there were some isolated reports of app crashes, indicating possible quality or stability issues.	LOW

Source Code Availability	Risk Level
The source code of the app is not publicly available, preventing a thorough review of the code. The inability to review the source code always poses a certain risk due to the potential for hidden malicious functionality.	MEDIUM

Third-Party Intelligence	Risk Level
External reports and other third-party sources have highlighted several serious vulnerabilities associated with the app, including possible exposure to malware and data breaches. Furthermore, there have been documented instances of successful exploitation of these vulnerabilities, leading to actual breaches in user data. These past breaches and existing vulnerabilities, combined with the potential severity of the associated risks, lead me to evaluate the risk level as High for this particular app.	HIGH
Recommendation	
Consult with the developer to understand their response to the documented vulnerabilities and their plan to mitigate these risks. The application should be updated to fix any known vulnerabilities before deployment.	

Methodology

The methodology applied in this assessment involved a comprehensive evaluation of the Android application using the Mobile Security Framework (MobSF). This dynamic and static analysis tool enabled a detailed inspection of the app's permissions, network activity, data encryption practices, and application components. Further manual analysis involved a review of app store records, source code availability, and insight into third-party intelligence.

Each of these areas were analysed meticulously to identify potential vulnerabilities and risks associated with the use of the application. The approach ensured a holistic review of the app, focusing not only on its functional aspects but also on its interaction with servers, the way it handles and transmits data, the permissions it requires, and the security controls surrounding its components.

Conclusion

Given the presence of multiple High risk factors, I strongly recommend a thorough review and mitigation of these risks before this application is approved for wider use within the organisation. More stringent controls over data handling and transmission, as well as a thorough review of permissions and third-party intelligence, are particularly crucial to address these concerns.