TikTok 16.6.43
com.zhiliaoapp.musically
67eed8ed76f58be7e462aeb8ac030fc6
AppInterrogator Version: 2.5.1
Scan Date: 07-13-2020

This Zimperium Executive Report contains a high-level summary and score for an app's identified risk conditions. This digest is intended for a non-technical audience and provides a synopsis of our findings. Each finding is represented by a Red or Orange color coded badge.

- A Red ring indicates a critical risk finding
- An Orange ring indicates a moderate risk

Security Summary

75/100
MED

The security summary focuses on risks contained in the application. These risks include (but are not limited to): risky functionality and code use, application capabilities, critical vulnerabilities and threats.

This app can load compiled code in APK and JAR files. This can include files located in external storage and potentially on the Internet.

The apps creates and launches a new subprocess outside of the calling app.

In inspecting the Android certificate for this application, other apps also use this certificate. The risks of all of these applications were examined to better understand if the apps built with this certificate contain similar risks.

This app uses system-level permissions dedicated for usage by system apps (like Android OS parts or device manufacturers installed ones).

This app implements the Intent 'StartService'. The Intent needs to either contain the complete class name of a specific service implementation, or a specific package name to target. Also, the calling service need to be listed in the Android manifest using the exported=false parameter to ensure that the calling service is not implicitly exported. Without this information leakage may occur.

Allows an application to request installing packages. Apps targeting APIs greater than 22 must hold this permission in order to use ACTION_INSTALL_PACKAGE.

This application can create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet. This is an informational finding.

This application can keep the device from going into sleep mode. If used improperly this could drain the device's power. This is an informational finding.

This application has the functionality to allow it to automatically start itself after a reboot. This is an informational finding.

This application can change how the account data is synced and backed up. This is an informational finding.

This application can move tasks to the foreground and background. This is an informational finding.

A pattern exists where the app has shutdown processes that it runs when it is terminated. The intent of these process needs be taken into consideration when quantifying this risk finding.

This application can authenticate through the accounts on the device. This permission allows the application to add and remove accounts, confirm credentials and retrieve access tokens. This is an informational finding.

This application can perform operations like adding and removing accounts, and deleting their password. This is an informational finding.

This application can control your audio settings such as volume levels. This is an informational finding.

The app sets the initial PRNG seed, and in certain cases where a fixed value or low entropy source is used, the resulting sequence can be predictable. The 'setseed' method is used to generate the seed and is not recommended. Best practices suggest an app allow the SecureRandom object to self-seed.

This app is using an RSA cipher without padding. There are several known attacks against unpadded RSA encryption.

Privacy Summary

61/100

MED

The privacy summary focuses on the application's access to privacy data, including (but not limited to): user data, contacts access, unique device identifiers, adware, SMS, and insecure storage of data and communications.

Content providers are implicitly not secure. They allow other applications on the device to request and share data. If sensitive information is accidentally leaked to a content provider, an attacker can call the content provider and the sensitive data is exposed to the attacker by the application.This is concerning because any third-party application containing malicious code does not require any granted permissions to obtain sensitive information from these applications.

This application has the permissions to list all the accounts on the device to include accounts created by other applications. This method returns personal and sensitive user data.

A URL was found with parameters that indicates the app potentially sends sensitive information.

This application can read from external storage mediums such as SD Cards. This is an informational finding.

This application can write to external storage such as an SD Card. This is an informational finding.

The application has access to the camera. Ensure it cannot take photo's without your knowledge. This is an information finding.

This application has the functionality to record audio with the microphone. This functionality could allow the app to record audio at any time and without notification. This is an informational finding.

This application can retrieve information about currently and recently running tasks. This may allow the app to discover information about other applications on the device. This is an informational finding.

The app writes information to the system log. This can result in unintended information leakage, however it cannot be automatically determined whether the logged data is sensitive.

The app has access to the BSSID, SSID, link speed, local MAC address, network id and local IP Address of the Wifi connection.

The app gets the saved password associated with the account.

This convenience helper combines the functionality of getAccountsByTypeAndFeatures.

This app can access and read the contents of the global clipboard.

This app can send a text based SMS message.

This application uses a method to retrieve the last known location of the device in the event that the location services are not available.

This app has access to the device microphone.

👤 The app accesses the address book and obtains the list of contacts.

OWASP Summary

4/10

FAIL

The OWASP summary contains the results of the testing that was performed on the application against the OWASP Top 10 Mobile categories. Sections that passed the testing are in green while sections that failed a test are highlighted in red.

M1: Improper Platform Usage

No problems found

M2: Insecure Data Storage

Content Providers are implicitly insecure. They allow other applications on the device to request and share data. If sensitive information is accidentally leaked in one of these content providers all an attacker needs to do is call the content provider and the sensitive data will be exposed to the attacker by the application.This is cause for concern as any 3rd party application containing malicious code does not require any granted permissions in order to obtain sensitive information from these applications.

The app writes information to the system log. This can result in unintended information leakage, however it cannot be automatically determined whether the logged data is sensitive.

M3: Insecure Communications

URL's were found embedded in the app that do not use a secure protocol. Applications should always use HTTPS connections when possible. Ensure sensitive data is not being sent over this insecure channel.

A URL was discovered with parameters that indicate it potentially sends sensitive information.

M4: Insecure Authentication

No problems found

M5: Insufficient Cryptography

The app sets the initial PRNG seed, and in certain cases where a fixed value or low entropy source is used, the resulting sequence can be predictable. The 'setseed' method is used to generate the seed and is not recommended. Best practices suggest an app allow the SecureRandom object to self-seed.

M6: Insecure Authorization

No problems found

M7: Client Code Quality

No problems found

M8: Code Tampering

No problems found

M9: Reverse Engineering

This application fails the Static Data Exposure test as outlined by OWASP Mobile Top 10.

This application fails the Source Code Reverse Engineering Exposure test as outlined by OWASP Mobile Top 10.

M10: Extraneous Functionality

No problems found