TikTok 166206
com.zhiliaoapp.musically
159d8e3d3ce9a8dbcb6d038812581bf2
Scan Engine Version: 4.8.27
Scan Date: 07-06-2020

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

Privacy Summary

98/100

HIGH

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.

This app attempts to retrieve a contact from the Address Book. The method ABAddressBookGetPersonWithRecordID was depreciated after IOS9.

This application has the functionality to take screenshots of the full UI, enabling an attacker to understand everything from installed apps to credentials.

The app implements a pin-point location functionality that Apple only allows in navigation apps. It can be considered geolocation abuse by Apple if implemented in non-navigation apps.

This application is actively monitoring and retrieving data from the iOS Pasteboard which can lead to the exposure of sensitive data which could potentially include credentials.

This application has the functionality to record audio.

This application uses a MobileCoreServices framework which enables the application to gain access to the Camera. How and when this feature is implemented within the app is important to quantifying this finding.

The app implements functionality that logs data to the system console. System log files are accessible to any app and could included PII data. The log files may also be shared with Apple.

The app is implementing functionality with the ability to record audio and video of the UI.

The app implements the AdMob advertising framework. AdMob is one of the world's largest mobile advertising platforms. The functionality will retrieve the device's MAC address which can be used by advertisers to track users across multiple applications without permission.

The app implements low-level API call to retrieve the device global Ad identifier key.

The app can use non-encrypted HTTP connections.

This app has functionality that allows it to communicate over non-secure http proxies.

The app implements Cloud-Base Storage through the CloudKit framework.

This app sends query parameters with private information such as the user.

This app sends query parameters with device information.

Security Summary

88/100

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.

HIGH

The authentication method 'NSURLAuthenticationMethodServerTrust' is being implemented. This authentication method can be used to override SSL and TLS chain validation.

The app is using the direct NSTask function to fork foreign processes. This is currently prohibited by Apple , the developer should consider using an approved Apple method to avoid this risk condition.

Access credentials (username/password) have been exposed in URL

The app may be vulnerable to local or remote SQL injection attack.

- Application implements a Listening Server over TCP Sockets
- The app will create a paired socket on the network.
- The app opens a networking listening port.
- The app is implementing network sockets. This is an informational finding.
- The app is configured to allow unsecure and unverified connections to servers with lower TLS cipher support. It will allow cipher suites that do not support forward secrecy and does not discriminate between HTTP or HTTPS connections.
- This app references the proxy API's in the CFNetwork Framework which can allow it to connect to a proxy or host a proxy service.
- The app is configured to allow unsecure and unverified connection to servers with lower TLS versions. It will allow cipher suites that do not support forward secrecy and does not discriminate between HTTP or HTTPS connections.
- This app is using API implementations that fail to properly validate SSL certificates. When a certificate is invalid or malicious, it might allow an attacker to spoof a trusted entity by using a Man-In-The-Middle (MITM) attack.
- 'Bearer' related oAuth (Open Authorization) tokens were found. An adversary could potentially gain access to these tokens if they are not encrypted.
- The app implements Swizzling API calls. This may impact the app's ability to trust security decisions that are based on untrusted inputs or manipulated/swizzled output.