



ZIMPERIUM[®]
MOBILE THREAT DEFENSE

Privacy and Security Issues Found in Popular Dating Apps




A Zimperium Analysis of 14 Top Mobile Dating Apps' Privacy and Security Risks

EXECUTIVE SUMMARY

In a first of its kind study, Zimperium investigated 14 of the leading mobile dating applications to understand how they manage users' security and privacy risks. The results are derived from Zimperium's advanced mobile application scanning service, [Zimperium z3A](#). z3A is a unique mobile security technology developed by and exclusively available to Zimperium customers.

Zimperium is providing the anonymous results of the mobile app risks to dating app providers, industry analysts and users. If you are a dating app developer/provider, Zimperium will assist you in identifying the privacy and security risks in your application.

As part of our study, mobile security researchers from the award-winning zLabs team assigned each application a grade:

-  **Passing:** The app has very few risks and does an above average job of protecting user data.
-  **Average:** The app has risks that need to be addressed and does an average job of protecting user data.
-  **Failing:** The app has significant risks and does a below average job of protecting user data.

Overall, iOS-based dating apps expose users to more privacy risks while Android-based apps have far more security issues.

Privacy Risks:

Scoring Summary:

100% of iOS-based apps and 71% of Android-based apps failed to receive a passing privacy grade.



Key Findings:

🍏 iOS:

- 100% (14 apps) log information into a system console; system log files (which may include PII) are accessible to any app.
- 100% (14 apps) can take screenshots of the full UI, enabling an attacker to understand everything from installed apps to credentials.
- 79% (11 apps) are actively monitoring and retrieving data from the iOS Pasteboard which can lead to exposure of data, potentially including credentials.

🤖 Android:

- 86% (12 apps) use an insecure content provider; this allows other applications (e.g., a malicious app) on the device to request and access data.

Security Risks:

Scoring Summary:

100% of iOS-based apps and 93% of Android-based apps failed to receive a passing security grade.

Key Findings:

🍏 iOS:

- 100% (14 apps) have an authentication method that can be used to override SSL and TLS chain validation.
- 100% (14 apps) implement Swizzling API calls which may impact the app's ability to trust security decisions that are based on manipulated/swizzled output.
- 43% (6 apps) allow unsecure and unverified connections to servers with lower TLS versions.
- 21% (3 apps) contain a Swizzling jailbreak method.

🤖 Android:

- 64% (9 apps) enable WebView to execute JavaScript code. This could potentially allow an attacker to introduce arbitrary JavaScript code to perform malicious actions.
- 50% (7 apps) have methods of injected Java objects that are enumerable from JavaScript.
- 50% (7 apps) can create new OS subprocess.
- 43% (6 apps) can execute commands at the OS level such as launching other applications and processes.



- 43% (6 apps) embed a version of the Facebook SDK which is vulnerable to session hijacking.
- 36% (5 apps) use WebKit to download a file from the Internet.
- 29% (4 apps) use insecure content providers that allow other apps on the device (potentially including ones containing malicious code) to request and share data.
- 29% (4 apps) have functionality to retrieve apps, Java code and DEX files from remote locations; allows the application to update and introduce additional code at any time.

The research team also analyzed each of the applications against the Open Web Application Security Project (OWASP) [Mobile Top 10](#) application development best practices. While the specifics are provided by iOS and Android below, there are some troubling issues that truly emerge when all 28 apps are considered together. For example:

- 96% (27 apps) are vulnerable to reverse engineering.
- 89% (25 apps) do not properly secure the communication of sensitive data.
- 82% (23 apps) do not properly store sensitive data.
- 50% (14 apps) are vulnerable to code tampering.

METHODOLOGY

This research details how both iOS and Android apps from 14 leading dating app providers fare when tested for security and privacy risks. Each app provider has been anonymized and assigned a pseudonym with a number, such as "Dating 8."

The scores are calculated using [Zimperium's z3A](#) Advanced Application Analysis engine. Zimperium z3A is the leading application reputation scanning service that continually evaluates risks posed by mobile apps.

z3A provides deep intelligence about app behavior, including content (the app code itself), intent (the app's behavior), and context (the domains, certificates, shared code, network communications, and other data). z3A also provides privacy and security ratings, enabling enterprises to create security policies limit or remove risky apps from managed devices.



This research scanned and scored the most recent versions of the 28 (14 iOS and 14 Android) mobile dating apps available in the Apple App Store and Google Play in January 2020.

There are three primary categories of analysis included for each app, and overall for the industry: Open Web Application Security Project (OWASP) Mobile Top 10 application development best practices and the more granular looks at privacy and security risks. The privacy and security scores are on a 0-100 scale. **Higher aggregate scores indicate apps that contain many privacy and security risk conditions.** Here is a summary of each report category:

- **OWASP Top 10 Summary:** The OWASP summary contains testing results performed on the application against the OWASP Top 10 Mobile best practices.
- **Privacy Risks:** The privacy information focuses on the application's access to private user data, unique device identifiers, SMS, communications, and unsecured data storage.
- **Security Risks:** The security summary focuses on application risks. These risks include functionality and code use, application capabilities, and critical vulnerabilities.

OWASP MOBILE TOP 10 RESULTS

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. OWASP publishes a top 10 list of application development best practices applying to web applications and a set applying to mobile apps.

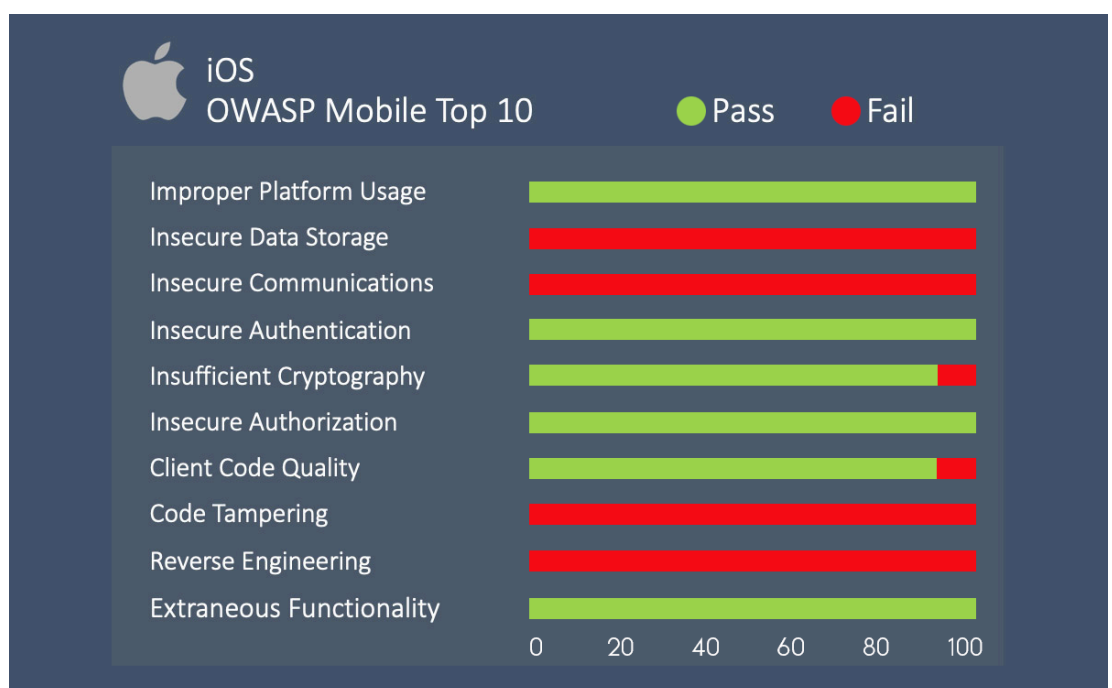
Part of our research into mobile dating apps includes providing a passing or failing mark for each of the OWASP Mobile Top 10. The tables that follow summarize passing and failing marks collectively for all of the apps on each platform. Sections receiving a passing mark are represented in green while sections failing a test are represented in red.

iOS

The OWASP results for iOS apps are fairly consistent across providers. There are five tests that 100% all iOS apps pass. There are also three tests that 100% fail and one that 97% fail.



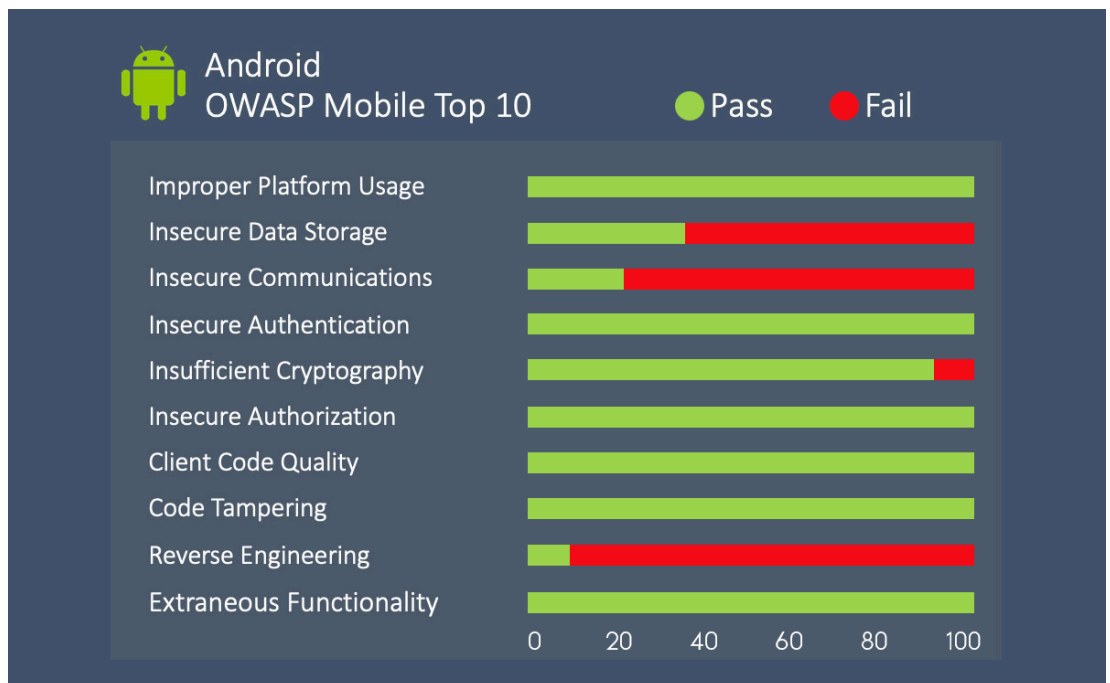
- 100% (14 apps) fail four tests, although often for different reasons. The failing tests are:
 - **M2: Insecure Data Storage.** The app is configured in a way that makes stored data potentially accessible by non-authorized parties.
 - **M3: Insecure Communications.** Someone could utilize network attacks to view and steal information in transit.
 - **M8: Code Tampering.** By tampering with the app directly, an attacker could view data and possibly create manipulated outputs (e.g., fraudulent transactions).
 - **M9: Reverse Engineering.** Someone could reverse engineer the apps to identify exploitable vulnerabilities to steal from customers or defraud users.
- 7% (1 app) fails to implement cryptography correctly (**M5: Insufficient Cryptography**). Known vulnerabilities exist with some cryptography functions and encryption/decryption routines. An attacker can use these published vulnerabilities and weaknesses to attack the encryption methods to decrypt and extract sensitive data.
- 7% (1 app) has code-level implementation problems in the mobile client (**M7: Code Quality**). Code-level implementation problems in the mobile client includes issues like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.



Android

The OWASP results for Android apps are less uniform than the iOS ones. While some of the failed tests are similar in nature to the iOS ones, the percentages are different and 100% of Android apps only fail one test. For brevity, the description impacts of the failed tests shared with iOS are not included, just the test name.

- 93% (13 apps) are vulnerable to reverse engineering (**M9: Reverse Engineering**).
- 79% (9 apps) fail to implement secure communications (**M3: Insecure Communications**).
- 64% (9 apps) fail to implement secure storage (**M2: Insecure Data Storage**).
- 7% (1 apps) fails to implement cryptography correctly (**M5: Insufficient Cryptography**).

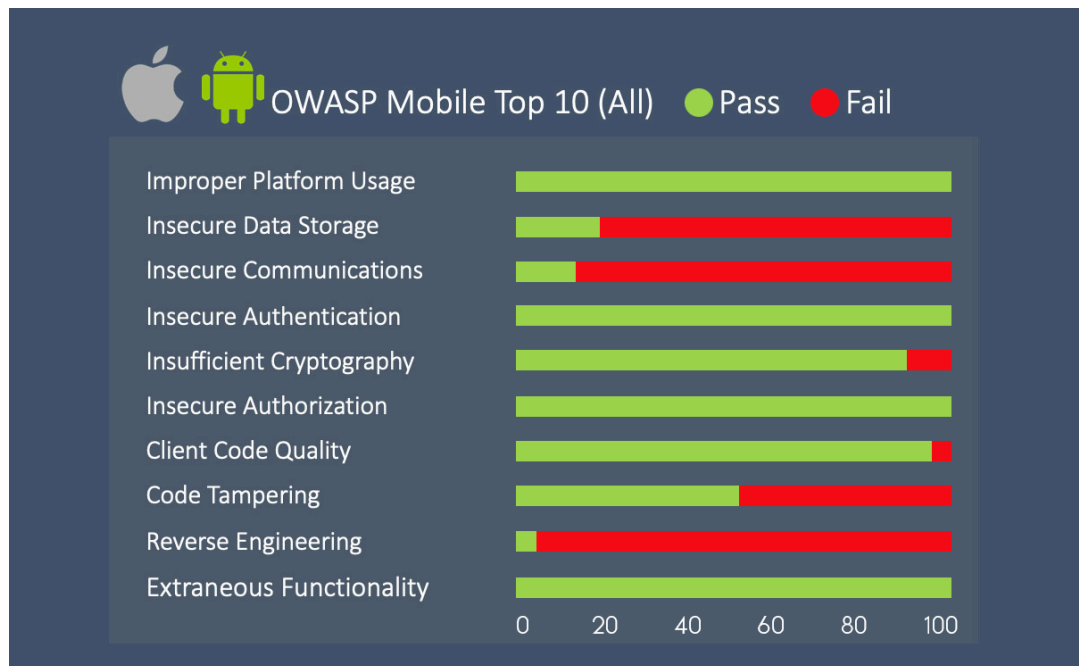


Overall

When examined across all 28 apps, some interesting trends emerge. For example, the majority of all apps are susceptible to attacks leveraging weaknesses highlighted by three tests (with a fourth just below a majority):

- 96% (27 apps) are vulnerable to reverse engineering (**M9: Reverse Engineering**).

- 89% (25 apps) fail to implement secure communications (**M3: Insecure Communications**).
- 82% (23 apps) fail to implement secure storage (**M2: Insecure Data Storage**).
- 50% (14 apps) are vulnerable to code tampering (**M8: Code Tampering**).

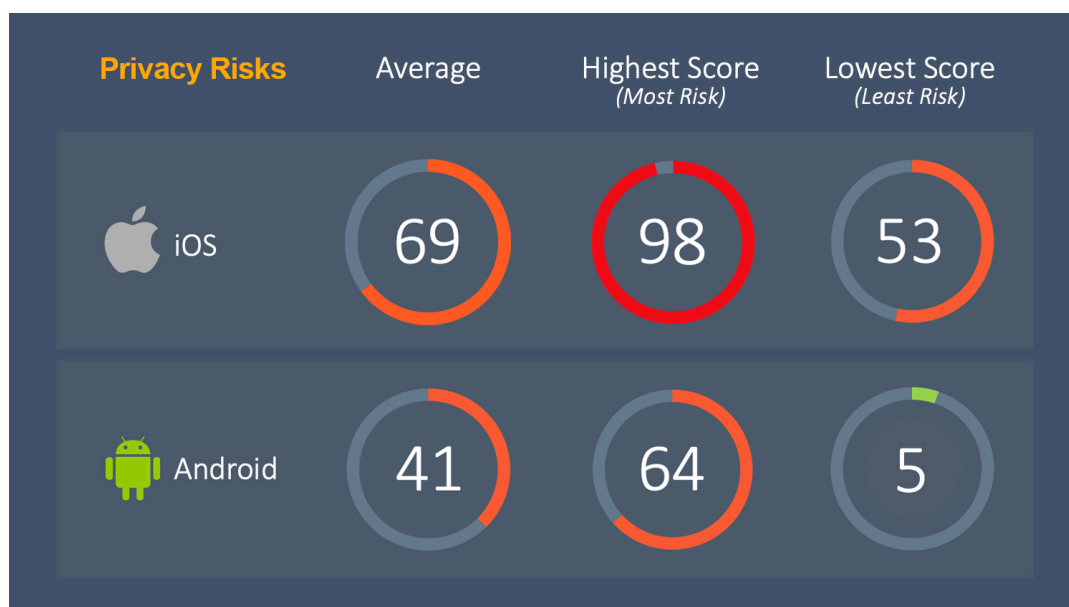


PRIVACY RISKS

Privacy assessments focus on apps' access to privacy data, including (but not limited to): user data, contacts, unique device identifiers, adware, SMS, and insecure storage of data and communications.

Here is a summary table of privacy scores using Zimperium's z3A Advanced Application Analysis for the 14 dating apps:





Taken as groups, neither iOS nor Android dating apps received a passing grade. However, as a group, Android apps were less risky from a privacy perspective than its iOS counterparts.

Not surprisingly, the iOS app scoring a 98 (very high privacy risk) has a large number of significant issues for privacy and data leakage. Here is a subset of those issues (impacts of which are outlined in the iOS Privacy section), including some that do not have any apparent legitimate use inside of a dating app:

- Logs information into a system console
- Can take screenshots of Full UI.
- Is actively monitoring the iOS Pasteboard.
- Includes advertising frameworks.
- Can view and import saved photos and videos.
- Can retrieve the device's MAC address.
- Can send SMS messages

The Android app scoring 64 (high privacy risk) has a different set of privacy risks (impacts of which are outlined in the Android Privacy section below) and also has capabilities that seem unnecessary for a dating app to include:

- Uses an insecure content provider.
- Contain exported components that could lead to data leakage.
- Retrieves the device's last known GPS coordinates.
- Can programmatically send SMS messages.
- Can create and share RSS feeds.
- Includes the Crashlytics SDK which can collect PII.

The major privacy risks in the iOS and Android versions are included in the respective sections.

Anonymous Name	🍏 iOS Privacy	🤖 Android Privacy	OVERALL Privacy
Dating 1	77	64	71
Dating 2	65	5	35
Dating 3	71	51	61
Dating 4	66	55	61
Dating 5	98	37	68
Dating 6	61	49	55
Dating 7	53	29	41
Dating 8	61	58	60
Dating 9	58	46	52
Dating 10	64	5	35
Dating 11	71	50	61
Dating 12	83	40	62
Dating 13	62	31	47
Dating 14	77	58	68
AVERAGE	69	41	55

PRIVACY RISKS - iOS

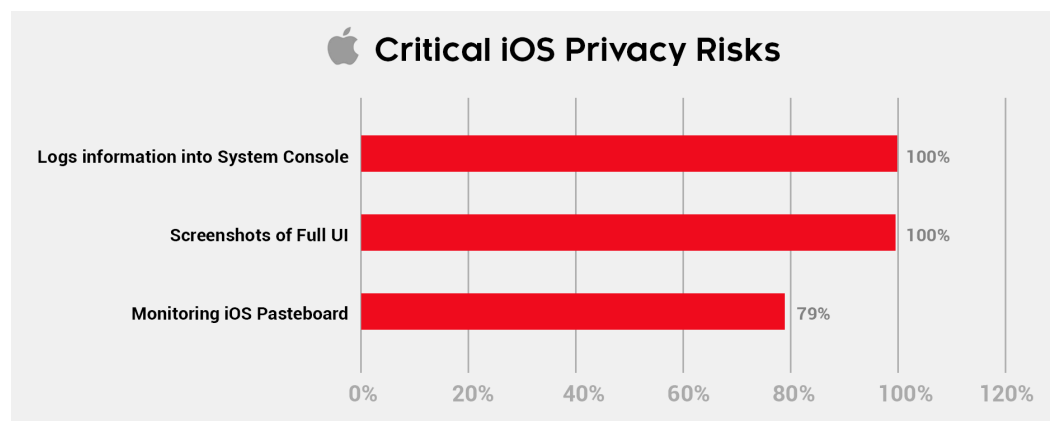
Analysis of iOS dating apps reveals 15 different major privacy issues, 3 of which are considered "critical." "Critical" issues are those that should be immediately addressed to prevent imminent data leakage (e.g., PII) or app rejection due to violating iOS/Android policies. "Dangerous" issues clandestinely expose users to ad networks or can be abused to capture data, recordings, photos, etc.

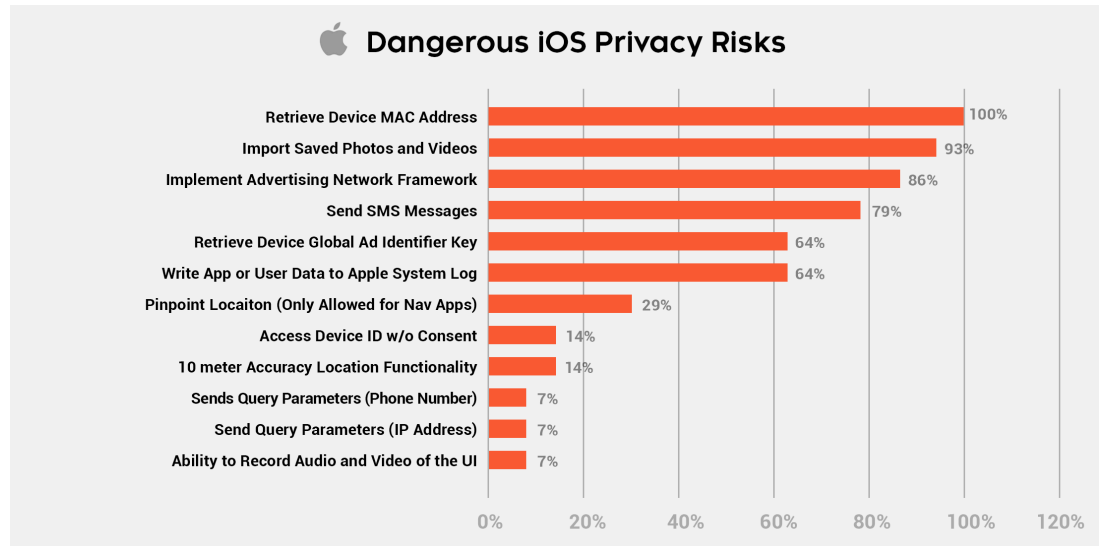


- All of the critical iOS privacy issues are shared by the majority of the apps:
 - 100% (14 apps) log information into a system console; system log files (which may include PII) are accessible to any app.
 - 100% (14 apps) can take screenshots of the full UI, enabling an attacker to understand everything from installed apps to credentials.
 - 79% (11 apps) are actively monitoring and retrieving data from the iOS Pasteboard which can lead to exposure of data, potentially including credentials.

- 7 major issues are shared by the majority of all iOS apps:
 - Critical:
 - 100% (14 apps) log information into a system console.
 - 10% (14 apps) can take screenshots of Full UI.
 - 79% (11 apps) are actively monitoring the iOS Pasteboard.
 - Dangerous:
 - 100% (14 apps) include advertising frameworks that clandestinely collect information about the user, the device and the app.
 - 93% (13 apps) can view and import saved photos and videos in the user's library, often without user consent.
 - 86% (12 apps) retrieve the device's MAC address which can be used by advertisers to track users across multiple applications without permission.
 - 79% (11 apps) can send SMS messages programmatically, potentially leading to unintentional data leakage or SMS spam.
 - 64% (9 apps) implement low-level API calls to retrieve the device global Ad identifier key.
 - 64% (9 apps) write app or user data to Apple system log that is accessible to all other apps allowing an attacker to easily dump device logs and retrieve any logged sensitive information.

Here are charts showing the critical and dangerous privacy risks in the 14 iOS dating apps:





PRIVACY RISKS - ANDROID

Overall, Android apps fared much better in privacy risk testing than their iOS counterparts. While analysis of Android apps reveals 14 different major privacy issues, two of which are considered critical, few apps contain multiple issues.

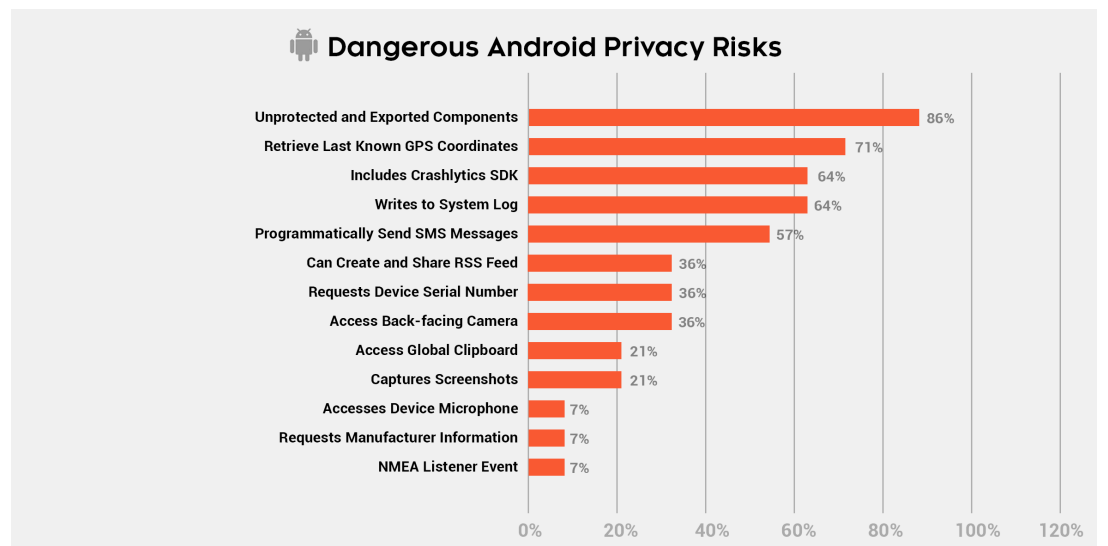
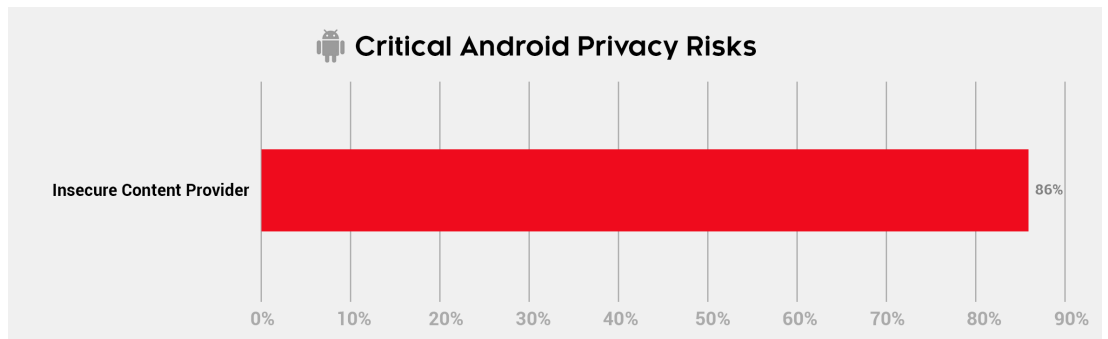


- There is one critical issue shared by multiple apps:
 - 86% (12 apps) use an insecure content provider; this allows other applications (e.g., a malicious app) on the device to request and access data.
- 6 major issues are shared by the majority of all Android apps:
 - Critical:
 - 86% (12 apps) use an insecure content provider.
 - Dangerous:
 - 86% (12 apps) contain exported components that are not protected by a permission. By starting and binding to the service, any app can leak information or perform unauthorized tasks.
 - 71% (10 apps) retrieve the device's last known GPS coordinates.
 - 64% (9 apps) write information to the system log which can result in unintended information leakage.
 - 64% (9 apps) include the Crashlytics SDK which can collect PII such as UUID, IP Address, name and email.



- 57% (8 apps) can send SMS messages programmatically, potentially leading to unintentional data leakage or SMS spam.

Here are charts showing the critical and dangerous privacy risks in the 14 Android dating apps:

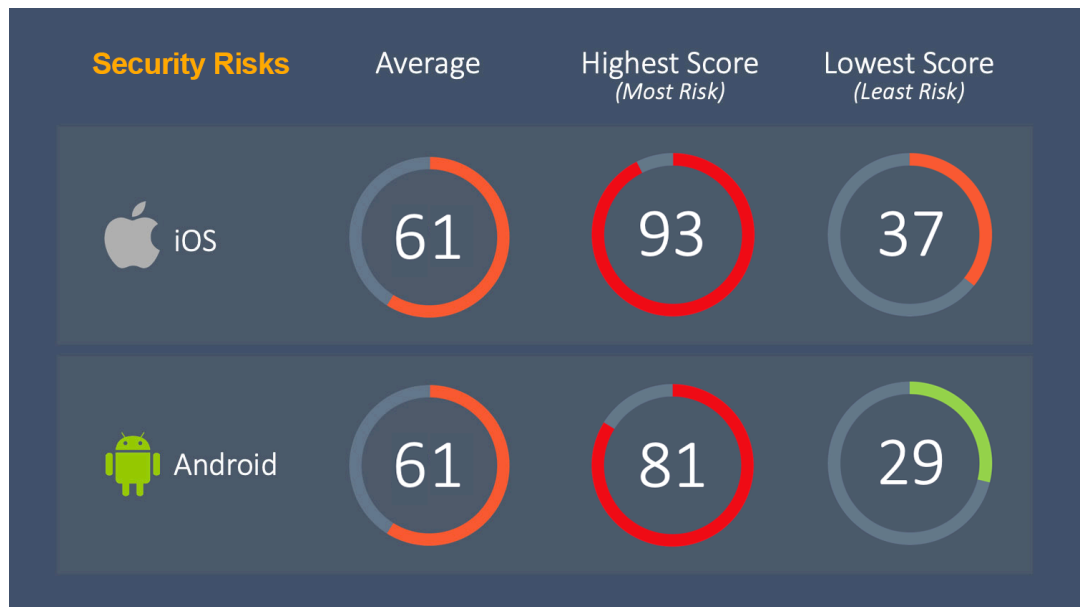


SECURITY RISKS

Security assessments focus on security holes and risks contained in the apps, including (but not limited to): risky functionality and code use, application capabilities, critical vulnerabilities and threats.



Here is a summary table of security scores using Zimperium's z3A Advanced Application Analysis for the 14 dating apps:



Despite the same average score, Android dating apps overall have more security risks than iOS ones.

The iOS app scoring 93 (very high security risks) has a large number of significant security issues (impacts of which are outlined in the iOS Security section below), including:

- Has an authentication method that can be used to override SSL and TLS chain validation.
- Implements Swizzling API calls.
- Allows unsecure and unverified connections to servers with lower TLS versions.
- Contain a Swizzling jailbreak method.
- May be vulnerable to local or remote SQL injection attacks.
- Has additional compiled libraries embedded in the app.
- Can use non-encrypted HTTP connections.

The Android app scoring 81 (very high security risks) is from the same provider and has a large number of significant security issues (impacts of which are outlined in the Android Security section), including:



- Enables WebView to execute JavaScript code.
- Has methods of injected Java objects that are enumerable from JavaScript.
- Can execute commands at the OS level.
- Retrieves apps, Java code & DEX files from remote locations.
- Does not validate SSL certificates.
- Has risky shutdown processes.
- Susceptible to code injection.

The security risks of the apps are included in the following sections:

Anonymous Name	iOS Security	Android Security	OVERALL Security
Dating 1	93	81	87
Dating 2	63	29	46
Dating 3	75	80	78
Dating 4	53	75	64
Dating 5	62	56	59
Dating 6	52	41	47
Dating 7	50	43	47
Dating 8	39	80	60
Dating 9	56	75	66
Dating 10	63	36	50
Dating 11	42	77	60
Dating 12	83	60	72
Dating 13	37	47	42
Dating 14	88	78	83
AVERAGE	61	61	61

SECURITY RISKS - iOS

Analysis of iOS dating apps reveals 15 different major security issues, six of which are considered "critical."

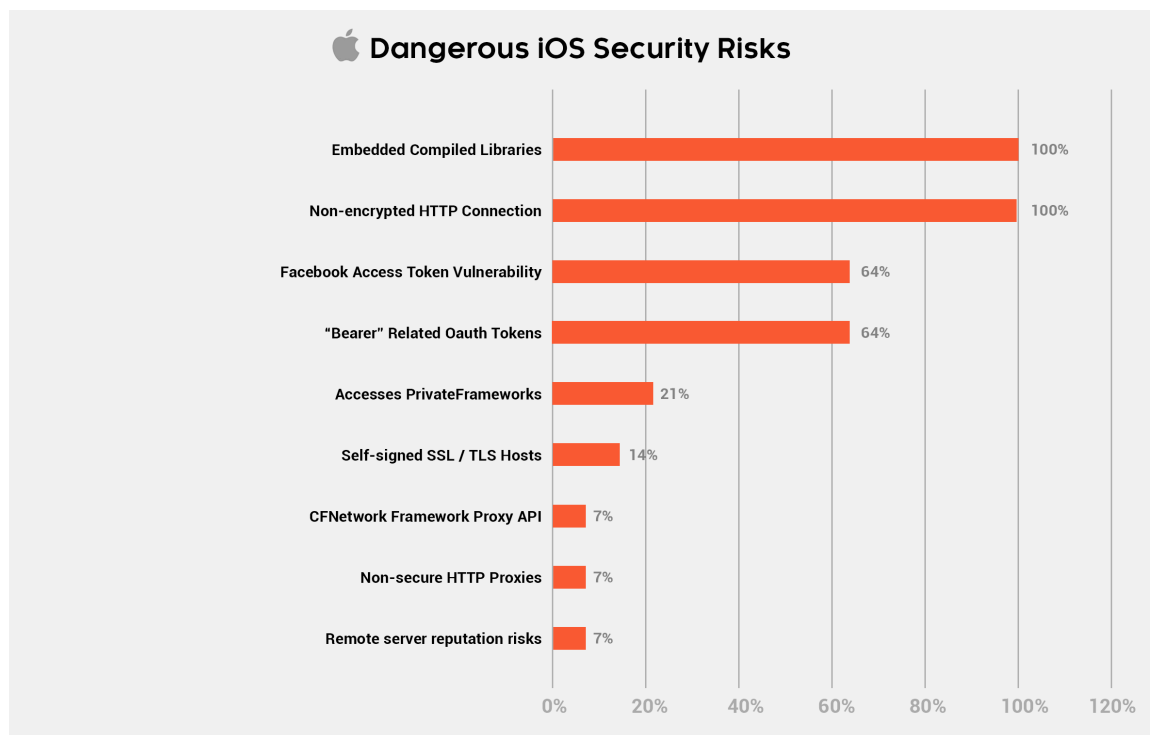
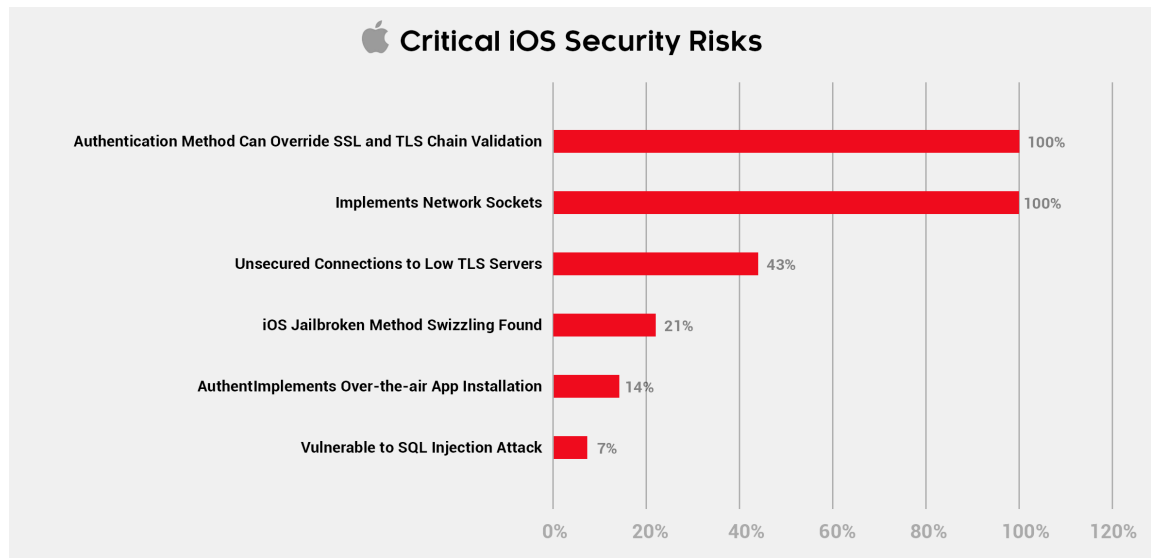
- Of the critical issues, all but one are shared by more than one app.
 - 100% (14 apps) have an authentication method that can be used to override SSL and TLS chain validation.
 - 100% (14 apps) implement Swizzling API calls which may impact the app's ability to trust security decisions that are based on manipulated/swizzled output.



- 43% (6 apps) allow unsecure and unverified connections to servers with lower TLS versions.
- 21% (3 apps) contain a Swizzling jailbreak method.
- 14% (3 apps) implement an over-the-air app installation method which circumvents Apple's review process and can install unapproved functionality.
- 7% (1 app) may be vulnerable to local or remote SQL injection attacks.
- 6 major issues are shared by the majority of all iOS apps:
 - Critical:
 - 100% (14 apps) have an authentication method that can override SSL and TLS chain validation.
 - 100% (14 apps) implement Swizzling API calls.
 - Dangerous:
 - 100% (14 apps) have additional compiled libraries embedded in the app which could unintentionally introduce additional security risks because the compiled code is from another developer.
 - 100% (14 apps) can use non-encrypted HTTP connections.
 - 64% (9 apps) contains the Facebook access token vulnerability. This means the authentication token key is being saved unencrypted to the file system. This impacts IOS 9 and below.
 - 64% (9 apps) contain 'Bearer' related oauth (Open Authorization) tokens; an adversary can gain access to these tokens if they are not encrypted.

Here are charts showing the critical and dangerous security risks in the 14 iOS dating apps:





SECURITY RISKS - ANDROID

Analysis of Android dating apps reveals 33 different major security issues, 11 of which are considered "critical."

- There are 11 critical Android security issues, all but three of which are shared by more than one app:

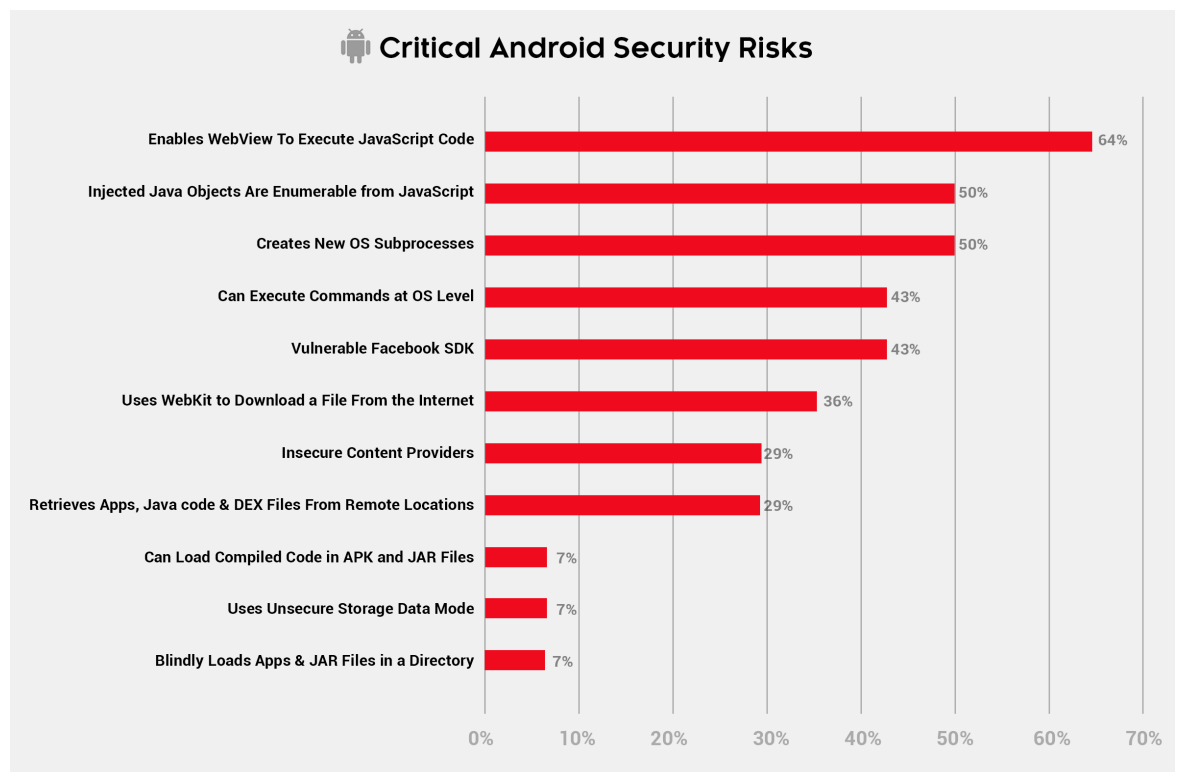


- 64% (9 apps) enable WebView to execute JavaScript code. This could potentially allow an attacker to introduce arbitrary JavaScript code to perform malicious actions.
 - 50% (7 apps) have methods of injected Java objects that are enumerable from JavaScript.
 - 50% (7 apps) can create new OS subprocess.
 - 43% (6 apps) can execute commands at the OS level such as launching other applications and processes.
 - 43% (6 apps) embed a version of the Facebook SDK which is vulnerable to session hijacking.
 - 36% (5 apps) use WebKit to download a file from the Internet.
 - 29% (4 apps) use insecure content providers that allow other apps on the device (potentially including ones containing malicious code) to request and share data.
 - 29% (4 apps) have functionality to retrieve apps, Java code and DEX files from remote locations; allows the application to update and introduce additional code at any time.
 - 7% (1 app) can load compiled code in APK and JAR files, including files located in external storage and potentially on the Internet.
 - 7% (1 app) uses unsecure storage data mode (WORLD_READABLE, WORLD_WRITABLE).
 - 7% (1 app) uses methods to blindly load all apps and JAR files located in a directory, enabling abuse by malicious parties.
- 7 major issues are shared by at least half of all Android apps:
 - Critical:
 - 64% (9 apps) enable WebView to execute JavaScript code. This could potentially allow an attacker to introduce arbitrary JavaScript code to perform malicious actions.
 - 50% (7 apps) have methods of injected Java objects that are enumerable from JavaScript.
 - 50% (7 apps) can create new OS subprocess.
 - Dangerous:
 - 79% (11 apps) are not actively validating SSL certificates.
 - 79% (11 apps) have shutdown processes that run when the app is terminated; during shutdown, the app could be storing credential data that can be exposed to an attacker.

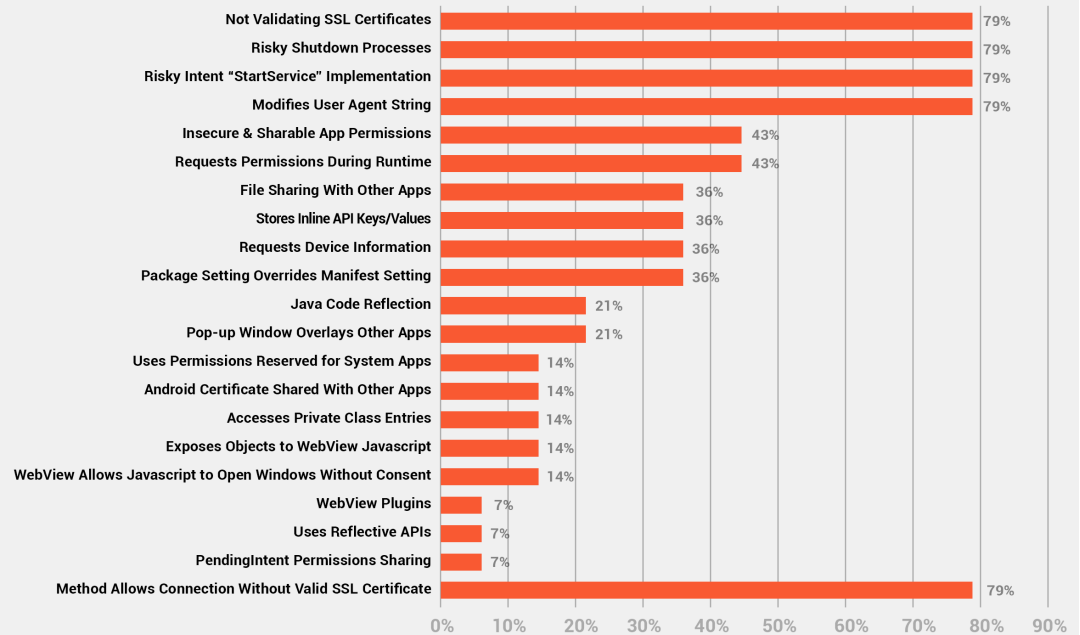


- 79% (11 apps) implement the Intent 'StartService' which can cause information leakage if not configured correctly.
- 79% (11 apps) modifies its user agent string; another app (potentially including a malicious one) using the same string may be able to communicate with the dating app's server.

Here are charts showing the critical and dangerous security risks in the 14 Android dating apps:



Dangerous Android Security Risks



CONCLUSION

Mobile dating apps are now the preferred and most popular way to find a potential date. Given the rapidly increasing usage and sensitivity of the information they contain, mobile dating apps need to constantly protect user information against security and privacy risks.

This research detailed how iOS and Android apps from 14 leading dating app providers protect users from security and privacy risks. The report outlined results in three primary categories: Open Web Application Security Project (OWASP) Mobile Top 10 application development best practices, privacy risks and security risks.

Overall, iOS-based dating apps expose users to more privacy risks while Android-based apps have far more security issues.

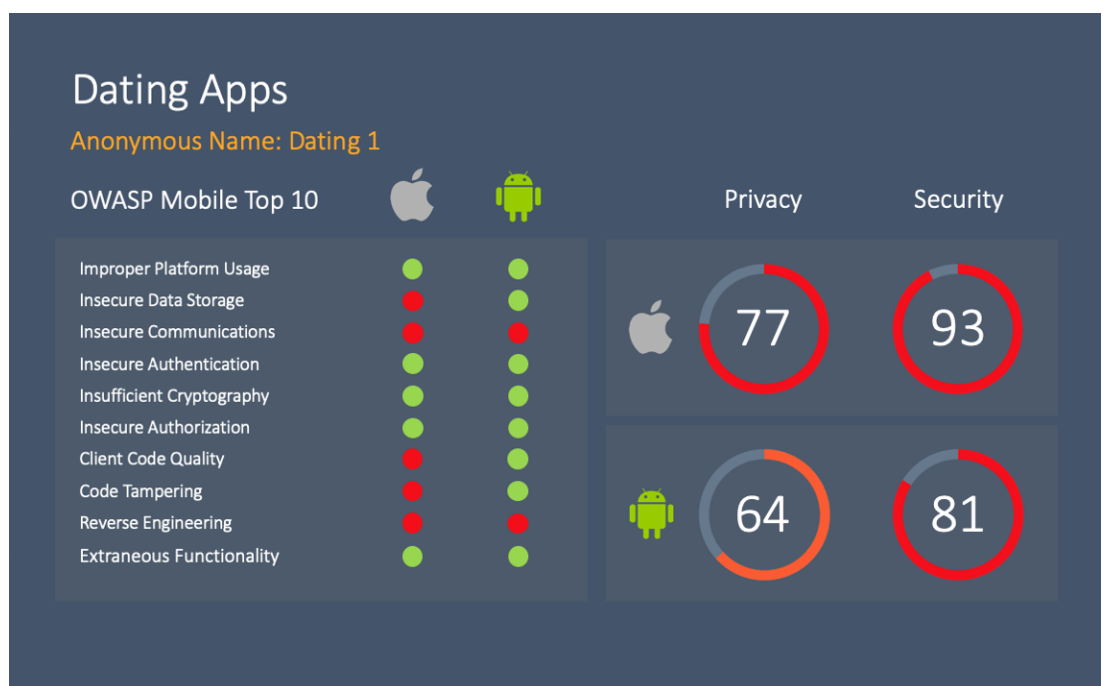
- **OWASP Top Ten:**

- iOS: The majority of iOS apps failed to receive a passing grade in four of the ten coding best practices.
- Android: The majority of Android apps failed to receive a passing grade in two of the ten coding best practices.

- **Privacy Risks:**
 - iOS: 100% of iOS-based apps failed to receive a passing privacy grade.
 - Android: 71% of Android-based apps failed to receive a passing privacy grade.
- **Security Risks:**
 - iOS: 100% of iOS-based apps failed to receive a passing security grade.
 - Android: 93% of Android-based apps failed to receive a passing security grade.

APPENDIX

The following are high-level summaries from the z3A application scans. Each dating app provider's iOS and Android apps are scanned independently. Each summary page greatly condenses the information from each report into a simple picture. Many z3A technical reports contain great detail and are more than 70 pages when printed. Each name is obfuscated in order to not identify the provider or its mobile apps. If you would like more information about your mobile application score, and how to build scanning of your apps into your development process to detect risks before the app is released, please [contact us](#) for a consultation.





Dating Apps

Anonymous Name: Dating 2

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 3

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality





Dating Apps

Anonymous Name: Dating 4

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 5

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality





Dating Apps

Anonymous Name: Dating 6

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 7

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality





Dating Apps

Anonymous Name: Dating 8

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 9

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality





Dating Apps

Anonymous Name: Dating 10

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 11

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality





Dating Apps

Anonymous Name: Dating 12

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 13

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality



Dating Apps

Anonymous Name: Dating 14

OWASP Mobile Top 10



Privacy

Security

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communications
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality

