



IOS STATIC ANALYSIS REPORT



🍏 \$(PRODUCT_NAME)
\$(MARKETING_VERSION))

File Name: ios.zip

Identifier: \$(PRODUCT_BUNDLE_IDENTIFIER)

Average CVSS Score: 7.5

App Security Score: 90/100 (LOW RISK)

Scan Date:

Dec. 5, 2020, 12:20 a.m.

FILE INFORMATION

File Name: ios.zip

Size: 1.29MB

MD5: 13295eff02a5448c05c3fa278413694e

SHA1: d6f8fa11042b592f35cbe0c55801efdbddc826db

SHA256: c1965033b6ce2d49219af91ef239cb843b653e7c30407d532a11eea6c769d46f

APP INFORMATION

App Name: \$(PRODUCT_NAME)

App Type: Swift

Identifier: \$(PRODUCT_BUNDLE_IDENTIFIER)

SDK Name:

Version: \$(MARKETING_VERSION)

Build: \$(CURRENT_PROJECT_VERSION)

Platform Version:

Min OS Version:

Supported Platforms:

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Used Realm database has configured encryption.	secure	CVSS V2: 0 (info) CWE: CWE-311 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-14	ios/BT/Storage/BTSecureStorage.swift
2	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 OWASP MASVS: MSTG-STORAGE-3	ios/BT/ExposureManager.swift
3	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ios/BT/Extensions/Foundation/StringExtensions.swift

URLs

URL	FILE
https://github.com/nh7a/Geohash/blob/master/Sources/Geohash/Geohash.swift https://www.movable-type.co.uk/scripts/geohash.html	ios/COVIDSafePaths/storage/Geohash.swift
https://developer.apple.com/documentation/exposurenotification/enmanager https://developer.apple.com/documentation/exposurenotification/enmanager/3583720-activate https://developer.apple.com/documentation/exposurenotification/enstatus/bluetoothtoothoff	ios/BT/ExposureManager.swift
http://stackoverflow.com/questions/24145838/querying-ios-keychain-using-swift/27721328#27721328	ios/BT/Storage/BTSecureStorage.swift
https://google.github.io/exposure-notifications-server/server_functional_requirements.html	ios/BT/API/Requests/DiagnosisKeyRequests.swift

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.

For every findings with severity **high** we reduce 15 from the score.

For every findings with severity **warning** we reduce 10 from the score.

For every findings with severity **good** we add 5 to the score.

If the calculated score is greater than 100, then the app security score is considered as 100.

And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.1.8 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2020 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).