



# 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:

March 5, 2021, 3:57 p.m.

## FILE INFORMATION

**File Name:** ios.zip

**Size:** 1.3MB

**MD5:** 9feec6b5bf1c48f9bb22e381a7a86e78

**SHA1:** 83eee3d39f6535880f01512b07a7929940c7604b

**SHA256:** f89b9fd15d7f20835a40b3f83eb97a12b41173dcfbd84b7e8a61c378eeef7a6

## 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	<b>CVSS V2: 0 (info)</b> CWE: CWE-311 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-14	ios/BT/Storage/BTSecureStorage.swift
2	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	<b>CVSS V2: 7.4 (high)</b> 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
3	The App logs information. Sensitive information should never be logged.	info	<b>CVSS V2: 7.5 (high)</b> CWE: CWE-532 OWASP MASVS: MSTG-STORAGE-3	ios/BT/ExposureManager.swift

## URLs

URL	FILE
<a href="https://github.com/nh7a/Geohash/blob/master/Sources/Geohash/Geohash.swift">https://github.com/nh7a/Geohash/blob/master/Sources/Geohash/Geohash.swift</a> <a href="https://www.movable-type.co.uk/scripts/geohash.html">https://www.movable-type.co.uk/scripts/geohash.html</a>	ios/COVIDSafePaths/storage/Geohash.swift
<a href="https://developer.apple.com/documentation/exposurenotification/enmanager">https://developer.apple.com/documentation/exposurenotification/enmanager</a> <a href="https://developer.apple.com/documentation/exposurenotification/enmanager/3583720-activate">https://developer.apple.com/documentation/exposurenotification/enmanager/3583720-activate</a>	ios/BT/ExposureManager.swift
<a href="https://developer.apple.com/documentation/exposurenotification/enexposuresummaryitem/3644417-weighteddurationsum">https://developer.apple.com/documentation/exposurenotification/enexposuresummaryitem/3644417-weighteddurationsum</a> ,	ios/BT/Extensions/Exposure Notifications/Scoring.swift
<a href="http://stackoverflow.com/questions/24145838/querying-ios-keychain-using-swift/27721328#27721328">http://stackoverflow.com/questions/24145838/querying-ios-keychain-using-swift/27721328#27721328</a>	ios/BT/Storage/BTSecureStorage.swift
<a href="https://forums.developer.apple.com/thread/113632">https://forums.developer.apple.com/thread/113632</a>	ios/EscrowVerification/Extensions/Extensions.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.

© 2021 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).