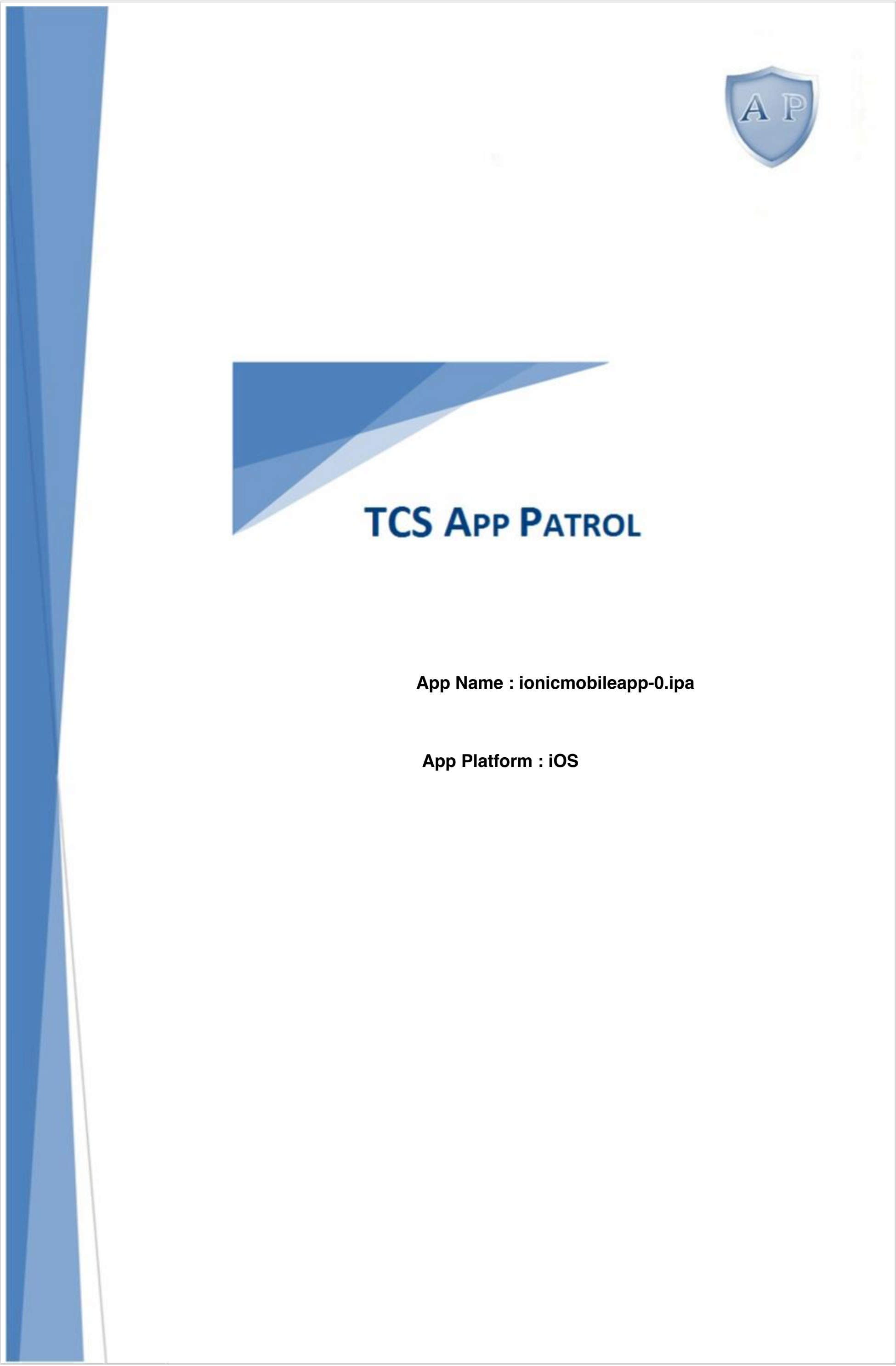

# TCS App Patrol

**App Name : ionicmobileapp-0.ipa**

**App Platform : iOS**

## CONFIDENTIALITY STATEMENT AND DISCLAIMER

This document contains information that is proprietary and confidential to Tata Consultancy Services Limited (TCS), which shall not be disclosed outside TI Security and, transmitted or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without express written permission of Tata Consultancy Services Limited (TCS) is prohibited. Any other company and product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

This report and any supplements are CONFIDENTIAL and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. If you are not the intended recipient, any use, disclosure, copying or distribution of the report is UNAUTHORIZED. If you have received this report in error, please destroy it immediately.

The Mobile Security tool App Patrol has a comprehensive knowledge of vulnerabilities which includes intelligence combined from OWASP Reference, Recent Threats and O.S. Platforms vulnerabilities. It should be understood that no amount of security assessment, in no mode and depth can expose all the innate security vulnerabilities. These types of assessments are intended to find the fundamental security issues within the assessment timeline. Thus it is highly recommended that even if select instances of issues are reported, the entire application be reviewed for these types of issues. App Patrol cannot be held liable for issues reported or not reported and for issues arising out of applying mitigation recommendations.

NOTE: The recommendation section provides developers, guidelines to mitigate vulnerabilities.

## File Summary

| Item | Value |
|---|---|
| Name | ionicmobileapp-0.ipa |
| Size | 16.73MB |
| MD5 | 8aeb64a3495454bf3e60def18de90c57 |
| SHA1 | e708c23b1699650f273e2c0421ef65f2b118376d |
| SHA256 | 1eda9dd4fd50e07d4387ead65e03cd2b32d35cf7d3b6e092b30ec099f8e64e52 |

## App Information

| Item | Value |
|---|---|
| App Name | ionicmobileapp |
| Identifier | com.tcs.mobility.etisalat |
| Version | 0.0.1 |
| SDK Name | iphoneos11.2 |
| Platform Version | 11.2 |
| Min OS Version | 10.0 |

## Permissions

| Permissions | Description | Reason in Manifest |
|---|---|---|
| NSLocationAlwaysUsageDescription | Access location information at all times. | This app wants to get your location always, even this app runs in background. |
| NSLocationAlwaysUsageDescription | Access location information at all times. | This app wants to get your location always, even this app runs in background. |
| NSLocationAlwaysUsageDescription | Access location information at all times. | This app wants to get your location always, even this app runs in background. |
| NSLocationWhenInUseUsageDescription | Access location information when app is in the foreground. | This app wants to get your location while this app runs only. |
| NSLocationWhenInUseUsageDescription | Access location information when app is in the foreground. | This app wants to get your location while this app runs only. |
| NSLocationWhenInUseUsageDescription | Access location information when app is in the foreground. | This app wants to get your location while this app runs only. |
| NSPhotoLibraryUsageDescription | Access the user's photo library. | This app requires photo library access to function properly. |
| NSPhotoLibraryUsageDescription | Access the user's photo library. | This app requires photo library access to function properly. |
| NSPhotoLibraryUsageDescription | Access the user's photo library. | This app requires photo library access to function properly. |

## App Transport Security

| Issue | Status | Description |
|---|---|---|
| Exception in NSAppTransportSecurity found. | Insecure | App Transport Security (ATS) is disabled on the domain '['127.0.0.1', 'accounts.google.com', 'akamaihd.net', 'api.facebook.com', 'fbcdn.net', 'graph.facebook.com', 'localhost', 'm.facebook.com', {'NSAllowsArbitraryLoads': True, 'NSExceptionDomains': {'127.0.0.1': {'NSExceptionAllowsInsecureHTTPLoads': True}, 'accounts.google.com': {}, 'akamaihd.net': {'NSIncludesSubdomains': True}, 'api.facebook.com': {}, 'fbcdn.net': {'NSIncludesSubdomains': True}, 'graph.facebook.com': {}, 'localhost': {'NSExceptionAllowsInsecureHTTPLoads': True}, 'm.facebook.com': {}}}]'. Disabling ATS can allow insecure communication with particular servers or allow insecure loads for web views or for media, while maintaining ATS protections elsewhere in your app. |

## Binary Analysis

| Issue | Status | Description |
|---|---|---|
| **fPIE -pie** flag is Found | Secure | App is compiled with Position Independent Executable (PIE) flag. This enables Address Space Layout Randomization (ASLR), a memory protection mechanism for exploit mitigation. |
| **fstack-protector-all** flag is Found | Secure | App is compiled with Stack Smashing Protector (SSP) flag and is having protection against Stack Overflows/Stack Smashing Attacks. |
| **fobjc-arc** flag is Found | Secure | App is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities. |
| Binary make use of banned API(s) | Insecure | The binary may contain the following banned API(s)<br>**_fopen, _alloca, _memcpy, _strlen, _stat, _sscanf, _vsnprintf, _gets** . |
| Binary make use of the following Crypto API(s) | Info | The binary may use the following crypto API(s)<br>**SecTrustEvaluate**. |
| Binary make use of the following Weak HASH API(s) | Insecure | The binary may use the following weak hash API(s)<br>**CC_MD5**. |
| Binary make use of the insecure Random Function(s) | Insecure | The binary may use the following insecure Random Function(s)<br>**_random, _srand**. |
| Binary make use of Logging Function | Info | The binary may use **NSLog** function for logging. |
| Binary make use of **malloc** Function | Insecure | The binary may use **malloc** function instead of **calloc**. |

## File analysis

| | |
|---|---|
| Plist Files | ionicmobileapp.app/Info.plist<br>ionicmobileapp.app/GoogleMaps.bundle/Info.plist<br>ionicmobileapp.app/GoogleMaps.bundle/GMSCoreResources.bundle/Info.plist<br>ionicmobileapp.app/GoogleMaps.bundle/GMSCacheStorage.momd/VersionInfo.plist<br>ionicmobileapp.app/CDVLaunchScreen.storyboardc/Info.plist |

# Appendix : Glossary

## 1. Risk Rating

| Severity | Description |
|---|---|
| High | The vulnerabilities under high rating are considered to be of highest risk level. Such vulnerability should be handled with highest priority. Under specific conditions, these vulnerabilities can potentially make the system unusable and lead to serious security breaches. |
| Medium | Though the threat is not critical at the moment, it has the potential to become a High risk threat in the future under certain circumstances if not mitigated. Medium risk vulnerabilities require significant mitigation to lower the impact of the threat. |
| Low | The information found is useful to the attacker, but is not a threat in itself. Existing security controls are likely to be adequate or the risk is acceptable, but over the period this may give rise to more serious problems. |
| Info | The data revealed is an additional piece of information and there are no serious security implications related to it. Items listed here are not vulnerabilities, but are indicators of overall application development security practices. |

| Risk Rating | | Impact | | |
|---|---|---|---|---|
| | | High | Medium | Low |
| Likelihood | High | High | High | Medium |
| | Medium | High | Medium | Low |
| | Low | Medium | Low | Info |

## 2. Vulnerability Title

The vulnerability title is a short one line description of the vulnerability discovered.

## 3. OWASP Reference

The OWASP reference is a standardized list of vulnerability types. This aims to identify each vulnerability type with a unique reference id, which may be used to access more information regarding the vulnerability.

## 4. Abstract

The section describes the severity of a potential attack based on successful exploitation of the vulnerability.

## 5. Vulnerability Description

The description gives the overview of flaw or bug that caused the vulnerability. This is a brief explanation of the vulnerability with examples.

## 6. Instance(s)

The section highlights vulnerabilities exist in Application scanned by plugin.

## 7. Recommendation

This section provides solutions or workarounds to mitigate the risk arising from this vulnerability.

## 8. Severity

The severity describes the risk level of the vulnerability.

## 9. Privacy Risk

Risk scoring of an application is based on the data obtained during risk analysis of application. Based on the data collected during the scan, the risk score is assigned to each risk and finally arrived at the overall score. The scan looks at the possible risks that an application can possess.

## 10. App Risk

This section rates the application based on the vulnerabilities and instances detected. A application is rated on a scale of 100 wherein the app with score in range 0 - 30 is under Low risk, 30 - 50 is under Medium risk, 50 and above is under High risk.

## 11. CVSS

The Common vulnerability scoring system CVSS is a NIST standard for assessing the severity of security vulnerabilities. The CVSS score establishes a measure of how much concern a vulnerability warrants, compared to other vulnerabilities. The score is arrived at considering various vectors and applying standard formulaes. The scores range from 0 to 10. Vulnerabilities with a base score in the range 7.0-10.0 are High, those in the range 4.0-6.9 as Medium, and 0-3.9 as Low.

**Reference**

www.first.org/cvss/cvss-guide

## 12. Compliance

An app must comply with privacy and data protection laws, regulations, and policies designed to protect confidential information, such as PCI DSS, NIST, HIPAA. This section provides an overview on which compliance has been violated by the app.

**PCI Reference**

https://www.pcisecuritystandards.org/index.php

**HIPPA Reference**

http://www.hhs.gov/ocr/privacy/

**NIST Reference**

http://csrc.nist.gov/publications/PubsSPs.html

**Document Reference**

https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CC0QFjAD&url=https%3A%2F%2Fcloudsecurityalliance.org%2Fguidance%2FCSA-ccm-v1.00.xlsx&ei=I6vhU82yEpK8ugSMzoDgCQ&usg=AFQjCNH50ajXlFyJ_Q5KMCyU16tlDJSYeg&bvm=bv.72197243,d.c2E