MOBSF

ANDROID STATIC ANALYSIS REPORT

I am Sober (1.1)

File Name:	I Am Sober_1.1_APKPure.apk
Package Name:	c.addictionrecoveryl.iamsober
Scan Date:	Nov. 17, 2024, 10:14 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	0	1	0

FILE INFORMATION

File Name: I Am Sober_1.1_APKPure.apk
Size: 1.43MB
MD5: 848c22390e242be196160e18957f56fb
SHA1: 96fd2a7a89d3e2641af904f300d3b907442fb3a4
SHA256: 578c100f75722d4484dba5927025813b837ed609b9cb2f34d23cff260a285ebe

APP INFORMATION

App Name: I am Sober
Package Name: c.addictionrecoveryl.iamsober
Main Activity: c.addictionrecoveryl.iamsober.MainActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 1.1
Android Version Code: 2

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-04-27 01:06:53+00:00
Valid To: 2049-04-27 01:06:53+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x77e702b63c5a6ee29063370ca17d2aa9846137b
Hash Algorithm: sha256
md5: a0e2e8abea50f54ed044519408a21503
sha1: de62e859019ee46f3a9febc19333965fa2e16634
sha256: 86f9053553949954afe3f94af884a0d94bca08a862dc9deedc98457b24ccd541
sha512: 54442efe80198ce14061975e2d5876a076eae2b523dc89e2ed4114eedcae3b0f26a355b5b9952f5d06409aa8fc14593fd292f316c642cb1b0f14ed2ab57d4400
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ecb8b03b3ced5a2e2368896f0a1980fdb7b46d3448575e47ff6a185bf08873df
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.1-4.1.2, [minSdk=16]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	1/25	android.permission.INTERNET
Other Common Permissions	0/44	

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.69.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
addictionrecoverycenter.strikingly.com	ok	**IP:** 54.192.51.48 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map

SCAN LOGS

Timestamp	Event	Error
2024-11-17 22:14:34	Generating Hashes	OK
2024-11-17 22:14:34	Extracting APK	OK

2024-11-17 22:14:34	Unzipping	OK
2024-11-17 22:14:34	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 22:14:34	Parsing APK with androguard	OK
2024-11-17 22:14:37	Parsing AndroidManifest.xml	OK
2024-11-17 22:14:37	Extracting Manifest Data	OK
2024-11-17 22:14:37	Performing Static Analysis on: I am Sober (c.addictionrecoveryl.iamsober)	OK
2024-11-17 22:14:37	Fetching Details from Play Store: c.addictionrecoveryl.iamsober	OK
2024-11-17 22:14:38	Manifest Analysis Started	OK
2024-11-17 22:14:38	Checking for Malware Permissions	OK
2024-11-17 22:14:38	Fetching icon path	OK
2024-11-17 22:14:38	Library Binary Analysis Started	OK

2024-11-17 22:14:38	Reading Code Signing Certificate	OK
2024-11-17 22:14:38	Running APKiD 2.1.5	OK
2024-11-17 22:14:39	Updating Trackers Database....	OK
2024-11-17 22:14:39	Detecting Trackers	OK
2024-11-17 22:14:40	Decompiling APK to Java with JADX	OK
2024-11-17 22:14:54	Converting DEX to Smali	OK
2024-11-17 22:14:54	Code Analysis Started on - java_source	OK
2024-11-17 22:14:54	Android SAST Completed	OK
2024-11-17 22:14:54	Android API Analysis Started	OK
2024-11-17 22:14:55	Android API Analysis Completed	OK
2024-11-17 22:14:57	Android Permission Mapping Started	OK

2024-11-17 22:14:58	Android Permission Mapping Completed	OK
2024-11-17 22:14:58	Email and URL Extraction Completed	OK
2024-11-17 22:14:58	Android Behaviour Analysis Started	OK
2024-11-17 22:14:59	Android Behaviour Analysis Completed	OK
2024-11-17 22:14:59	Extracting String data from APK	OK
2024-11-17 22:14:59	Extracting String data from Code	OK
2024-11-17 22:14:59	Extracting String values and entropies from Code	OK
2024-11-17 22:15:00	Performing Malware check on extracted domains	OK
2024-11-17 22:15:01	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.