MOBSF

ANDROID STATIC ANALYSIS REPORT

sisport_app (1.0.0)

File Name:	app.apk
Package Name:	com.example.sisport_app
Average CVSS Score:	7.0
App Security Score:	55/100 (MEDIUM RISK)
Scan Date:	April 16, 2021, 6:52 a.m.

FILE INFORMATION

File Name: app.apk
Size: 49.35MB
MD5: c19b736b14beb5a2eca1e561d24b85d0
SHA1: 03b7be79c429572662881d9af7e7c94cc320ab93
SHA256: e1d40bc4bcb353518347d0780d697e936d45c3974d747ae7ab05e80319d0d177

APP INFORMATION

App Name: sisport_app
Package Name: com.example.sisport_app
Main Activity: com.example.sisport_app.MainActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-02-24 22:50:37+00:00
Valid To: 2051-02-17 22:50:37+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: 1738dc364a3282b0cb8959a80f4a05ce
sha1: 19625f266d61dab021668e0fa16c4cb46a68f378
sha256: b03ecff3a7f160978b9ecb5e98b36a749d2d031d2a59407ff784a2f94ec6c7b1
sha512: 881ddd105a2115b5c9283b6524bbbfb027883c55119a8e12e20dd494b4a84918dca3711facd674454604eaa93119de3524c84aa7b8fbcfee77650e83f76c39e2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 50911148ffeca86eae0c71cb063ccab2e887ffd644023547c07ce0f291ce1e34

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0
bad	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
bad	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

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: DETAILS Anti-VM Code: Build.MANUFACTURER check Compiler: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 None (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/common/StandardMessageCodec.java io/flutter/embedding/engine/FlutterEnginePluginRegistry.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java io/flutter/view/FlutterView.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterSplashView.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java kotlin/io/ConsoleKt.java io/flutter/plugin/common/EventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/view/AccessibilityBridge.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/dart/DartExecutor.java io/flutter/plugin/platform/PlatformPlugin.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/view/FlutterNativeView.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/Log.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/FlutterException.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/android/AndroidKeyProcessor.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 None (info) OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.java
3	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 None (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java
4	The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 None (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	kotlin/random/PlatformRandom.java kotlin/random/AbstractPlatformRandom.java kotlin/random/KotlinRandom.java kotlin/random/FallbackThreadLocalRandom$implStorage$1.java kotlin/random/PlatformRandomKt.java kotlin/random/FallbackThreadLocalRandom.java kotlin/collections/CollectionsKt__MutableCollectionsJVMKt.java
5	App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	kotlin/io/FilesKt__UtilsKt.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortifed functions: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/x86/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86_64/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortifed functions: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk', '__vsprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.
9	FCS_CKM_EXT.1.1	Selection-Based Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
developer.android.com	good	**IP:** 172.217.8.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
github.com	good	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
www.w3c.orghttp	good	No Geolocation information available.

URLS

URL	FILE
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/PlatformViewsController.java
https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects	io/flutter/view/FlutterView.java
http://www.w3.org/XML/1998/namespace data:application/dart data:application/dart; http://www.w3.org/2000/xmlns/ https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). http://www.w3c.orghttp://dev.w3.org/CSS/fonts/ahem/COPYING data:/)){var data:text/javascript;charset=utf-8, http://www.w3.org/1999/xhtml	lib/arm64-v8a/libflutter.so

URL	FILE
http://www.w3.org/XML/1998/namespace data:application/dart data:application/dart; http://www.w3.org/2000/xmlns/ https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). http://www.w3c.orghttp://dev.w3.org/CSS/fonts/ahem/COPYING data:/)){var data:text/javascript;charset=utf-8, http://www.w3.org/1999/xhtml	lib/x86/libflutter.so
data:application/dart data:application/dart; https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). http://www.w3.org/XML/1998/namespace http://www.w3.org/2000/xmlns/ http://www.w3c.orghttp://dev.w3.org/CSS/fonts/ahem/COPYING data:/)){var data:text/javascript;charset=utf-8, http://www.w3.org/1999/xhtml	lib/x86_64/libflutter.so

EMAILS

EMAIL	FILE
appro@openssl.org	lib/arm64-v8a/libflutter.so

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 v3.1.9 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.