MOBSF

ANDROID STATIC ANALYSIS REPORT

Sieve (1.0)

File Name:	sieve (1).apk
Package Name:	com.mwr.example.sieve
Scan Date:	June 16, 2022, 10:30 a.m.
App Security Score:	29/100 (CRITICAL RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
10	10	2	1	1

FILE INFORMATION

File Name: sieve (1).apk
Size: 0.35MB
MD5: b011baaa8aac34fbdf68691e63a96a08
SHA1: 1017a046cd963d7be05c7d6302de48c94b4c6850
SHA256: 31878e33c526f9747c9b7ff38954bfcb2acc2a947ce7103589438e034637a6b7

APP INFORMATION

App Name: Sieve
Package Name: com.mwr.example.sieve
Main Activity: .MainLoginActivity
Target SDK: 17
Min SDK: 8
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 8
Services: 2
Receivers: 0
Providers: 2
Exported Activities: 2
Exported Services: 2
Exported Receivers: 0
Exported Providers: 2

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-12-10 16:13:17+00:00
Valid To: 2042-12-03 16:13:17+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x8cb1ba3
Hash Algorithm: sha256
md5: a8890569c57dccd72705995bbe2b411d
sha1: 1901fb7891bfc127363701812b81735e3ee3de08
sha256: dca76ba76f4b3f5dea55952a5e85670fb7fbd298fe4ae6f2ca4b5b6aba0df5c1
sha512: 74745fcd32bb24280cc20500ba17a5f8570a3a04910ef744367072d699f4d4df66c9355bfdd260d87c29ae7daa83c556b60abac08afe61e0b72540f31f073ae1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	android.permission.READ_EXTERNAL_STORAGE is not a subelement of the . These elements would not take effect	warning	The parent element of <permission>can only be <manifest>, or these definition and declearation would not take effect.

NO	ISSUE	SEVERITY	DESCRIPTION
2	android.permission.WRITE_EXTERNAL_STORAGE is not a subelement of the . These elements would not take effect	warning	The parent element of <permission>can only be <manifest>, or these definition and declearation would not take effect.
3	android.permission.INTERNET is not a subelement of the . These elements would not take effect	warning	The parent element of <permission>can only be <manifest>, or these definition and declearation would not take effect.
4	com.mwr.example.sieve.READ_KEYS is not a subelement of the . These elements would not take effect	warning	The parent element of <permission>can only be <manifest>, or these definition and declearation would not take effect.
5	com.mwr.example.sieve.WRITE_KEYS is not a subelement of the . These elements would not take effect	warning	The parent element of <permission>can only be <manifest>, or these definition and declearation would not take effect.
6	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.
7	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.
8	Activity (.FileSelectActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Launch Mode of Activity (.MainLoginActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Activity (.PWList) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Service (.AuthService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Service (.CryptoService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Content Provider (.DBContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Content Provider (.FileBackupProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on 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	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/mwr/example/sieve/CryptoServiceConnector.java com/mwr/example/sieve/ShortLoginActivity.java com/mwr/example/sieve/PWList.java com/mwr/example/sieve/NetBackupHandler.java com/mwr/example/sieve/MainLoginActivity.java com/mwr/example/sieve/CryptoService.java com/mwr/example/sieve/AuthService.java com/mwr/example/sieve/SettingsActivity.java com/mwr/example/sieve/AddEntryActivity.java com/mwr/example/sieve/FileBackupProvider.java com/mwr/example/sieve/DBParser.java com/mwr/example/sieve/AuthServiceConnector.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/mwr/example/sieve/ShortLoginActivity.java com/mwr/example/sieve/PWList.java com/mwr/example/sieve/PWTable.java com/mwr/example/sieve/WelcomeActivity.java com/mwr/example/sieve/MainLoginActivity.java com/mwr/example/sieve/CryptoService.java com/mwr/example/sieve/AuthService.java com/mwr/example/sieve/SettingsActivity.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/mwr/example/sieve/PWList.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/mwr/example/sieve/SettingsActivity.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mwr/example/sieve/SettingsActivity.java
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/mwr/example/sieve/PWDBHelper.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi/libencrypt.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 This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None 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 fortify functions.	True info Symbols are stripped.
2	lib/armeabi/libdecrypt.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 This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None 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 fortify functions.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided 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	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
9	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
10	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
11	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
12	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
13	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map

---

Report Generated by - MobSF v3.5.2 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.