MOBSF

ANDROID STATIC ANALYSIS REPORT

tapXphone (1.6.1)

File Name:	pay3.apk
Package Name:	by.iba.tapxphone
Scan Date:	May 25, 2022, 10:18 a.m.
App Security Score:	67/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	1	2	2

FILE INFORMATION

File Name: pay3.apk
Size: 24.1MB
MD5: f8332619da0537909c7f8547d330e05a
SHA1: 5f2fbbe490440d0f3b471b9b760e11be28187c9b
SHA256: 766ada64063cab5fe2ffc792c850881c125bb82282e8e521aa16d909588d89f9

APP INFORMATION

App Name: tapXphone
Package Name: by.iba.tapxphone
Main Activity: .ui.activities.MainActivity
Target SDK: 31
Min SDK: 26
Max SDK:
Android Version Name: 1.6.1
Android Version Code: 243

APP COMPONENTS

Activities: 26
Services: 1
Receivers: 0
Providers: 1
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: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-23 15:02:05+00:00
Valid To: 2050-03-23 15:02:05+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xeae719f322271d5501053c1382398aa0519f4786
Hash Algorithm: sha256
md5: 719ece5623087cfca5e74679a8b803d6
sha1: 5a279b834a2509230748e90e2e3f964f39377821
sha256: d54a904abaad268c5b68ce089da60f056ace26337b6e505f1323d94a1f852737
sha512: a794d0ac738cf3794a3975ea75236f0ee6a9523f6797582add59e822923c3ea60174a4ead2aca63cafe3ed37d71b1d5232e02a9d9090ad24661cdcc8e75131b2
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: b188b317b8be004ff136f8ecd4b55fca363828f335c90ea54e5c21a7152fa4fd

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/C1083du.java o/setValidator.java o/AB.java o/lambda$setListeners$2$SettingActivity.java o/getComment.java o/setAccessibilityHeading.java o/C1937ue.java o/setLeftEdgeEffectColor.java o/lambda$setListeners$0$PanEnterActivity.java o/C0049Bb.java o/setOutlineSpotShadowColor.java o/setDesignInformation.java o/setImportantForContentCapture.java o/C0121Dv.java o/getFrameDuration.java o/CX.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/CX.java o/setCurrentItem.java o/setBaselineAlignBottom.java o/setFirstBaselineToTopHeight.java o/setLayoutTransition.java o/setTextureWidth.java o/setDropDownWidth.java o/setTitleTextColor.java o/lambda$setListeners$0$ActivityAbout.java o/setDrawFullUnderline.java o/setLastVerticalBias.java o/setCompoundDrawablesRelative.java o/setLayoutDirection.java o/getNativeErrorCode.java o/CS.java o/AbstractC1987vb.java o/getSecureRandom.java o/lambda$setListeners$0$ConfirmLicenceActivity.java o/setX.java o/ActivityC1886tg.java o/C1941ui.java o/getPathData.java o/C0179Gb.java o/setMargin.java o/setOffscreenPageLimit.java o/CK.java o/setTouchscreenBlocksFocus.java o/getRemoteContext.java o/isRestrictedUserProfile.java o/setMaxLines.java o/lambda$setListeners$3$ActivityAbout.java o/setInputMethodMode.java o/lambda$setListeners$3$TransactionListActivity.java o/C2039wa.java o/C2101xj.java o/setPropertyName.java o/View$OnClickListenerC0114Do.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/AR.java o/lambda$setListeners$6$CardAttachActivity.java o/AbstractC0047Az.java o/setScrollbarFadingEnabled$ComponentActivity$5.java o/lambda$setListeners$0$ChooseCountryActivity.java o/C0092Cs.java o/aaP.java o/setOnPageChangeListener.java o/RunnableC2167yw.java o/lambda$setClickListeners$6$EnterAmountActivity.java o/setIconified.java o/C2110xs.java o/unregisterForContextMenu.java o/setImeOptions.java o/ActivityC1895tp.java o/lambda$setListeners$5$ChangePassActivity.java o/C2137yS.java o/lambda$setListeners$4$ActivityAbout.java o/setLayoutInflater.java o/lambda$setListeners$1$ChooseCountryActivity.java o/setDrawerElevation.java o/C0738acd.java o/C0024Ac.java o/setOnClickListener.java o/lambda$setListeners$3$ConfirmLicenceActivity.java o/setDividerDrawable.java o/setIcon.java o/jniInit1.java o/C2152yh.java o/setLastVerticalStyle.java o/lambda$setListeners$8$LoginActivity.java o/setColorFilter.java

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	o/getHeight.java o/TC.java o/setStrokeWidth.java o/honorsDebugCertificates.java o/BinderC2092xa.java o/Scope.java o/C1940uh.java o/setScaleX.java o/setScaleY.java o/setTextDirection.java o/View$OnClickListenerC1950ur.java o/readObject.java o/setDescendantFocusability.java o/onActivityDestroyed.java o/AbstractC0060Bm.java o/ActivityC1913uG.java o/setTextSelectHandle.java o/setEnabled.java o/AbstractC1926uT.java o/RunnableC2064wz.java o/setHorizontalStyle.java o/setScrollbarFadingEnabled.java o/setOnFocusChangeListener.java o/setDuplicateParentStateEnabled.java o/setInteractionEnabled.java o/HandlerC2048wj.java o/setVerticalAlign.java o/C0103Dd.java o/C2013wA.java o/setImageBitmap.java o/AF.java o/getCurrentLoop.java o/C1081ds.java o/CE.java o/BinderC2123yE.java o/FragmentContainerView.java o/setNextFocusRightId.java o/GifInfoHandle.java o/DC.java o/setIndicatorBoundsRelative.java o/C1991vf.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/setViewTranslationCallback.java o/setLinksClickable.java o/C2102xk.java o/BR.java o/setSupportImageTintMode.java o/C1075dl.java o/setTextClassifier.java o/lambda$setListeners$9$LoginActivity.java o/setDropDownBackgroundDrawable.java o/AO.java o/AbstractDialogInterface$OnClickListenerC2193zV.java o/BK.java o/AbstractC1924uR.java o/lambda$setClickListeners$7$EnterAmountActivity.java o/C2057ws.java o/RemoteActionCompat.java o/setCheckMarkTintList.java o/setFontFeatureSettings.java o/setBackgroundTintMode.java o/extractNativeFileDescriptor.java o/lambda$setListeners$1$SettingActivity.java o/setPictureListener.java o/HandlerC2093xb.java o/setOnGroupExpandListener.java o/setEllipsize.java o/lambda$setListeners$5$PanEnterActivity.java o/setImageURI.java o/IconCompat.java o/lambda$setListeners$0$CabinetActivity.java o/setElegantTextHeight.java o/setHint.java o/AbstractC2089xX.java o/lambda$setListeners$3$PanEnterActivity.java o/lambda$setListeners$5$CardAttachActivi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ty.java o/setContentPadding.java o/C1082dt.java o/lambda$setClickListeners$0$MenuActivity.java o/AbstractC2130yL.java o/lambda$setListeners$2$SignatureActivity.java o/lambda$setListeners$9$PinEnterActivity.java o/setOnHide.java o/C0086Cm.java o/getLoopCount.java o/Scope$ComponentActivity$3.java o/setOnCapturedPointerListener.java o/C0501Ue.java o/C2107xp.java o/C2210zm.java o/C0046Ay.java o/lambda$setListeners$1$LoginActivity.java o/getCurrentFrameIndex.java o/AE.java o/setRightEdgeEffectColor.java o/SavedStateRegistry$1.java o/C2049wk.java o/C2122yD.java o/setPopupBackgroundResource.java o/setLinkTextColor.java o/HandlerC2042wd.java o/safeJNIexchange.java o/setSplitTrack.java o/setButtonTintBlendMode.java o/lambda$setListeners$1$CabinetActivity.java o/C1966vG.java o/setOverScrollMode.java o/setSaveEnabled.java o/C0056Bi.java o/C2188zQ.java o/setPaddingTop.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/setTranslationZ.java o/setOnCheckedChangeListener.java o/enableUsingApkIndependentContext.java o/setMovementMethod.java o/setNextFocusLeftId.java o/setAddStatesFromChildren.java o/setPageTransformer.java o/lambda$setListeners$0$ChooseAcquirerActivity.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	o/AbstractC0581Xg.java o/C0585Xk.java o/AbstractC1051dN.java o/ActivityC1886tg.java o/C0371Nm.java o/C0586Xl.java o/C0436Rr.java o/C0440Rv.java o/C0584Xj.java o/setIcon.java o/C0583Xi.java o/C0754act.java o/C0706aaz.java o/acB.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	o/abY.java o/abR.java o/abT.java o/C1124ei.java o/abX.java
4	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	o/getRemoteContext.java o/setPropertyName.java by/iba/tapxphone/jni/JNIHandler.java o/aiD.java o/getRemoteResource.java o/C0909aim.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	o/C0877ahh.java o/C0514Ur.java o/FC.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	o/FragmentContainerView.java
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	o/C0844agb.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/liba.so	False high The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as 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.	No 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	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		False high	False high	No RELRO high	None info	None info	False warning	True info
2	lib/x86/liba.so	The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.	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.	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.	The shared object does not have run-time search path or RPATH set.	The shared object does not have RUNPATH set.	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.	Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/arm64-v8a/liba.so	False high The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as 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.	No 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	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		False high	False high	No RELRO high	None info	None info	False warning	True info
4	lib/x86_64/liba.so	The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.	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.	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.	The shared object does not have run-time search path or RPATH set.	The shared object does not have RUNPATH set.	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.	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 implement 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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'NFC', '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 implement functionality to encrypt sensitive data in non-volatile memory.
8	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
9	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.
10	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.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
16	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 142.251.39.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.googleapis.com	ok	**IP:** 216.58.214.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0099gì@ÿ.2eeú	o/setInputExtras.java
u0013android@android.com0 u0013android@android.com	o/CO.java

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.