MOBSF

ANDROID STATIC ANALYSIS REPORT

HappyMod (3.1.6c)

File Name: HappyMod-3-1-5.apk

Package Name:	com.happymod.apk
Scan Date:	March 18, 2025, 3:54 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	15	0	2	1

FILE INFORMATION

File Name: HappyMod-3-1-5.apk
Size: 17.41MB
MD5: 3e4a8dee7dfe5c6313180a96a77c8682
SHA1: 18e5efceecbf8c0e1988cb9c67d1c7ecdc805d73
SHA256: ce05bd64b09199dfb21a10aa297ce65361b370c166627c28b1cd2658da49da9b

APP INFORMATION

App Name: HappyMod
Package Name: com.happymod.apk
Main Activity: com.happymod.apk.hmmvp.main.LaunchActivity
Target SDK: 31
Min SDK: 21
Max SDK:
Android Version Name: 3.1.6c
Android Version Code: 252

APP COMPONENTS

Activities: 80
Services: 14
Receivers: 13
Providers: 4
Exported Activities: 5

Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: O=evz
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-03-15 08:11:53+00:00
Valid To: 2118-02-19 08:11:53+00:00
Issuer: O=evz
Serial Number: 0x3dec09c4
Hash Algorithm: sha256
md5: eb3c6564a7a7f8332a98bd9c139822d4
sha1: 8f16d0f9eab6ffb4ccef615c7a6b015210e09b1f
sha256: c3846f1b45b579e694f13553f5d7ae45615bac95647f8ed8bd76c9153ef4e0d3
sha512: ffd66a930cb8cce569d41b5887693b60007b1d5cf3206d61a201999a3717402f27e97303ab6ce4a5622f5bc671c16f1862cd4899ac003ac27b685c887573936a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: caa9a620c516e161eb33edc349a203b28c641e6ccbbcd8140fb69c8ce8368e3f
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
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.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.FOREGROUND_SERVICE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.happymod.apk.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
3e4a8dee7dfe5c6313180a96a77c8682.apk	FINDINGS: Packer Found — DETAILS: Mobile Tencent Protect Tencent's Legu
classes2.dex	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes3.dex	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
<tr><td>Anti Disassembly Code</td><td>non-zero link size
non-zero link offset</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.happymod.apk.hmmvp.allfunction.JumpProtocolActivity	Schemes: happymod://,
com.happymod.apk.hmmvp.allfunction.JumpHptActivity	Schemes: modupdate://, Hosts: starthm, Paths: /detail,
com.happymod.apk.hmmvp.allfunction.JumpHM	Schemes: gamecallback://, Hosts: route, Paths: /detail,

ACTIVITY	INTENT
com.happymod.apk.hmmvp.allfunction.JumpInstallerActivity	Schemes: file://, content://, Hosts: *, Mime Types: */*, application/xapk, application/xapk.1, application/xapk.1.1, application/xapk.1.1.1, application/xapk.1.1.1.1, application/xapk.1.1.1.1.1, Path Patterns: .*\\.xapk, .*\\..*\\.xapk, .*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk, .*\\.bapk, .*\\..*\\.bapk, .*\\..*\\..*\\.bapk, .*\\..*\\..*\\..*\\.bapk, .*\\..*\\..*\\..*\\..*\\.bapk, .*\\..*\\..*\\..*\\..*\\..*\\.bapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.bapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.bapk, .*\\.apkm, .*\\..*\\.apkm, .*\\..*\\..*\\.apkm, .*\\..*\\..*\\..*\\.apkm, .*\\..*\\..*\\..*\\..*\\.apkm, .*\\..*\\..*\\..*\\..*\\..*\\.apkm, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.apkm, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.apkm, .*\\.apks, .*\\..*\\.apks, .*\\..*\\..*\\.apks, .*\\..*\\..*\\..*\\.apks, .*\\..*\\..*\\..*\\..*\\.apks, .*\\..*\\..*\\..*\\..*\\..*\\.apks, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.apks, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.apks, .*\\.sapk, .*\\..*\\.sapk, .*\\..*\\..*\\.sapk, .*\\..*\\..*\\.sapk, .*\\..*\\..*\\..*\\.sapk, .*\\..*\\..*\\..*\\..*\\.sapk, .*\\..*\\..*\\..*\\..*\\..*\\.sapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.sapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.sapk, .*\\.xapk.*, .*\\..*\\.xapk.*, .*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk.*,

NETWORK SECURITY

HIGH: 1 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
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: 1 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
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.
4	Activity (com.happymod.apk.hmmvp.allfunction.JumpProtocolActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (btdownload.gui.view.TorrentGetActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.happymod.apk.hmmvp.allfunction.JumpHptActivity) is not Protected. [android:exported=true]	warning	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
7	Activity (com.happymod.apk.hmmvp.allfunction.JumpHM) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.happymod.apk.hmmvp.allfunction.JumpInstallerActivity) is not Protected. [android:exported=true]	warning	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	Broadcast Receiver (btdownload.services.EngineBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Service (btdownload.services.statistics.WorkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Service (com.liulishuo.filedownloader.services.FileDownloadService$SharedMainProcessService) is not Protected. [android:exported=true]	warning	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 (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/wrapper/proxyapplication/WrapperProxyApplication.java
2	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/example/helloworld/BuildConfig.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libjlibtorrent-1.2.15.2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__write_chk', '__strchr_chk', '__strlen_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libshell-super.com.happymod.apk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libshella-4.6.2.2.so	False high The binary 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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 RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libjlibtorrent-1.2.15.2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__write_chk', '__strchr_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libshell-super.com.happymod.apk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libshella-4.6.2.2.so	False high The binary 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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 RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libjlibtorrent-1.2.15.2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__write_chk', '__strchr_chk', '__strlen_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libshell-super.com.happymod.apk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libshella-4.6.2.2.so	False high The binary 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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 RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi-v7a/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi-v7a/libjlibtorrent-1.2.15.2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__write_chk', '__strchr_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	armeabi-v7a/libshell-super.com.happymod.apk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	armeabi-v7a/libshella-4.6.2.2.so	False high The binary 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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 RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	armeabi-v7a/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/libHappymodPrincess.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libCSTAMP.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/wrapper/proxyapplication/AndroidNClassLoader.java com/wrapper/proxyapplication/MultiDex.java com/wrapper/proxyapplication/MultiDexForTinker.java com/wrapper/proxyapplication/Util.java
00013	Read file and put it into a stream	file	com/wrapper/proxyapplication/Util.java
00012	Read data and put it into a buffer stream	file	com/wrapper/proxyapplication/Util.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/379613389119/namespaces/firebase:fetch?key=AIzaSyDSXPSa8tDX7dsVnTFizTYBZ0ZsUP4-Y5Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.CAMERA, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK
Other Common Permissions	5/44	com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
schemas.xmlsoap.org	ok	**IP:** 13.107.246.72 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyDSXPSa8tDX7dsVnTFizTYBZ0ZsUP4-Y5Q"
"Username" : "Lietotājvārds"

POSSIBLE SECRETS
"Resetpassword" : "□□□□"
"Username" : "□□□□□"
"Username" : "■■■■■■■■"
"Password" : "heslo"
"repliedtouser" : "□□"
"Password" : "Parola"
"repliedtouser" : "geantwortet"
"repliedtouser" : "απάντησε"
"Password" : "□□□□□"
"Password" : "Zaporka"
"Username" : "■■■■■■■■■■■■"
"Password" : "пароля"
"Password" : "■■■■■■■■■■■"
"Password" : "□□"
"Password" : "Contraseña"
"Password" : "■■■■■■■■■■"
"Username" : "Gebruikersnaam"

POSSIBLE SECRETS
"Username" : "■■■■■■■■■■■■■"
"repliedtouser" : "ענה"
"Password" : "Wachtwoord"
"Password" : "■■■■■■■■■"
"Password" : "□□"
"repliedtouser" : "■■■■■■"
"Username" : "□□□"
"Password" : "■■■■■■"
"com.google.firebase.crashlytics.mapping_file_id" : "eefd30286e0f4ac8844f2ac109f7aefe"
"Username" : "Username"
"Password" : "■■■■■■■■■"
"Password" : "Лозинка"
"repliedtouser" : "■■■■■■■■■■■■"
"Password" : "Hasło"
"Username" : "Felhasználónév"
"Password" : "Jelszó"
"Resetpassword" : "□□□□"

POSSIBLE SECRETS
"Password" : "Senha"
"repliedtouser" : "□□"
"Username" : "Nutzername"
"Password" : "fjalëkalim"
"Password" : "■■■■■■■"
"Password" : "Parole"
"google_api_key" : "AIzaSyDSXPSa8tDX7dsVnTFizTYBZ0ZsUP4-Y5Q"
"Username" : "■■■■■■■■■■"
"dyStrategy.privateAddress" : "privateAddress"
"Password" : "Passwort"
"Password" : "Heslo"
"Password" : "□□"
"Resetpassword" : "□□□□□□□□□□□□"
"Password" : "Password"
"Password" : "סיסמה"
"repliedtouser" : "válaszolt"
"Password" : "■■■■■■■■"

POSSIBLE SECRETS
"Password" : "пароль"
"repliedtouser" : "odpovedal"
"Username" : "Потребител"
"Enteryourpassword" : "6□8□□"
"Enteryourpassword" : "6-8□□□"
"Username" : "■■■■■■■■■■"
"repliedtouser" : "□□□□□"
"repliedtouser" : "■■■■■■■"
"Resetpassword" : "■■■■■■■■■■■■■■■"
"Password" : "■■■■■■■"
"Username" : "□□□"
"Enteryourpassword" : "6-8□□□"

SCAN LOGS

Timestamp	Event	Error
2025-03-18 03:54:14	Generating Hashes	OK

2025-03-18 03:54:14	Extracting APK	OK
2025-03-18 03:54:14	Unzipping	OK
2025-03-18 03:54:14	Parsing APK with androguard	OK
2025-03-18 03:54:15	Extracting APK features using aapt/aapt2	OK
2025-03-18 03:54:15	Getting Hardcoded Certificates/Keystores	OK
2025-03-18 03:54:17	Parsing AndroidManifest.xml	OK
2025-03-18 03:54:17	Extracting Manifest Data	OK
2025-03-18 03:54:17	Manifest Analysis Started	OK
2025-03-18 03:54:17	Reading Network Security config from network_security_config.xml	OK
2025-03-18 03:54:17	Parsing Network Security config	OK
2025-03-18 03:54:17	Performing Static Analysis on: HappyMod (com.happymod.apk)	OK
2025-03-18 03:54:17	Fetching Details from Play Store: com.happymod.apk	OK

2025-03-18 03:54:17	Checking for Malware Permissions	OK
2025-03-18 03:54:17	Fetching icon path	OK
2025-03-18 03:54:17	Library Binary Analysis Started	OK
2025-03-18 03:54:17	Analyzing apktool_out/lib/arm64-v8a/libHappymodPrincess.so	OK
2025-03-18 03:54:17	Analyzing apktool_out/lib/arm64-v8a/libjlibtorrent-1.2.15.2.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/arm64-v8a/libshell-super.com.happymod.apk.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/arm64-v8a/libshella-4.6.2.2.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/arm64-v8a/libCSTAMP.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/armeabi-v7a/libHappymodPrincess.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/armeabi-v7a/libjlibtorrent-1.2.15.2.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/armeabi-v7a/libshell-super.com.happymod.apk.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/armeabi-v7a/libshella-4.6.2.2.so	OK

2025-03-18 03:54:18	Analyzing apktool_out/lib/armeabi-v7a/libCSTAMP.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/x86/libHappymodPrincess.so	OK
2025-03-18 03:54:18	Analyzing apktool_out/lib/x86/libCSTAMP.so	OK
2025-03-18 03:54:18	Analyzing lib/arm64-v8a/libHappymodPrincess.so	OK
2025-03-18 03:54:18	Analyzing lib/arm64-v8a/libjlibtorrent-1.2.15.2.so	OK
2025-03-18 03:54:18	Analyzing lib/arm64-v8a/libshell-super.com.happymod.apk.so	OK
2025-03-18 03:54:18	Analyzing lib/arm64-v8a/libshella-4.6.2.2.so	OK
2025-03-18 03:54:18	Analyzing lib/arm64-v8a/libCSTAMP.so	OK
2025-03-18 03:54:18	Analyzing lib/armeabi-v7a/libHappymodPrincess.so	OK
2025-03-18 03:54:18	Analyzing lib/armeabi-v7a/libjlibtorrent-1.2.15.2.so	OK
2025-03-18 03:54:18	Analyzing lib/armeabi-v7a/libshell-super.com.happymod.apk.so	OK
2025-03-18 03:54:18	Analyzing lib/armeabi-v7a/libshella-4.6.2.2.so	OK

2025-03-18 03:54:18	Analyzing lib/armeabi-v7a/libCSTAMP.so	OK
2025-03-18 03:54:18	Analyzing lib/x86/libHappymodPrincess.so	OK
2025-03-18 03:54:18	Analyzing lib/x86/libCSTAMP.so	OK
2025-03-18 03:54:18	Reading Code Signing Certificate	OK
2025-03-18 03:54:18	Running APKiD 2.1.5	OK
2025-03-18 03:54:21	Updating Trackers Database....	OK
2025-03-18 03:54:21	Detecting Trackers	OK
2025-03-18 03:54:22	Decompiling APK to Java with JADX	OK
2025-03-18 03:54:24	Converting DEX to Smali	OK
2025-03-18 03:54:24	Code Analysis Started on - java_source	OK
2025-03-18 03:54:24	Android SBOM Analysis Completed	OK
2025-03-18 03:54:27	Android SAST Completed	OK

2025-03-18 03:54:27	Android API Analysis Started	OK
2025-03-18 03:54:31	Android API Analysis Completed	OK
2025-03-18 03:54:31	Android Permission Mapping Started	OK
2025-03-18 03:54:34	Android Permission Mapping Completed	OK
2025-03-18 03:54:34	Android Behaviour Analysis Started	OK
2025-03-18 03:54:37	Android Behaviour Analysis Completed	OK
2025-03-18 03:54:37	Extracting Emails and URLs from Source Code	OK
2025-03-18 03:54:37	Email and URL Extraction Completed	OK
2025-03-18 03:54:37	Extracting String data from APK	OK
2025-03-18 03:54:38	Extracting String data from SO	OK
2025-03-18 03:54:38	Extracting String data from Code	OK
2025-03-18 03:54:38	Extracting String values and entropies from Code	OK

2025-03-18 03:54:38	Performing Malware check on extracted domains	OK
2025-03-18 03:54:41	Saving to Database	OK

Report Generated by - MobSF v4.3.1

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.