MobSF

ANDROID STATIC ANALYSIS REPORT

DroidFS (2.2.0)

File Name:	sushi.hardcore.droidfs_374.apk

Package Name:	sushi.hardcore.droidfs
Scan Date:	Aug. 1, 2025, 1:21 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	11	1	1	1

FILE INFORMATION

File Name: sushi.hardcore.droidfs_374.apk
Size: 9.53MB
MD5: cf75b784807d60e647ce762c238c05e8
SHA1: 96dd29977110fb81af900b152bce4875d3f264a9
SHA256: d5f08dd612decfd0c99f2f33640cd029dd6cf892be065ff8950b91a339db7a59

APP INFORMATION

App Name: DroidFS
Package Name: sushi.hardcore.droidfs
Main Activity: sushi.hardcore.droidfs.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 2.2.0
Android Version Code: 374

APP COMPONENTS

Activities: 14
Services: 4
Receivers: 2
Providers: 3
Exported Activities: 0
Exported Services: 0

Exported Receivers: 1
Exported Providers: 2

✹ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-03-21 22:53:30+00:00
Valid To: 2048-08-06 22:53:30+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x7076c437d328fdb4
Hash Algorithm: sha256
md5: 73bed0ee42f62aa7d4b624bdfbb2e888
sha1: 9082ce498447e78f760f5f40ebc3224be8c1b65f
sha256: 1b8934d493310a342b29bbe03bc205e0d3d58659d1abaf179577d947452499d6
sha512: 872b53ce7e17f3115012c7793376168f09c3a1a8042a67364a06dc90f779e314bec9bab1f375504a3b5b786b26f0e0a2075318b105c57ff6513aacb6cd39c7bc
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ff303b4c9f91bc9578dab5bb4d10acaffa69b8d4da3175bb235874a92358aa8e
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
sushi.hardcore.droidfs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched 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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	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.
3	Content Provider (sushi.hardcore.droidfs.content_providers.TemporaryFileProvider) is not Protected. [android:exported=true]	warning	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.
4	Content Provider (sushi.hardcore.droidfs.content_providers.VolumeProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.MANAGE_DOCUMENTS [android:exported=true]	warning	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. 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.
5	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: **0** | WARNING: **5** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

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	app/grapheneos/pdfviewer/loader/DocumentPropertiesAsyncTaskLoader.java com/bumptech/glide/Glide.java com/bumptech/glide/RequestBuilder.java com/bumptech/glide/RequestManager.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/engine/ActiveResources.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/Jobs.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/executor/GlideExecutor$UncaughtThrowableStrategy$2.java com/bumptech/glide/load/model/AssetUriLoader.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/UnitModelLoader.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/CenterInside.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsamp

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifFrameResourceDecoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/SingletonConnectivityReceiver$FrameworkConnectivityMonitorPreApi24.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/ViewTarget$SizeDeterminer.java com/bumptech/glide/util/ByteBufferUtil.java com/bumptech/glide/util/pool/FactoryPools.java sushi/hardcore/droidfs/CameraActivity$onClickTakePhoto$1.java sushi/hardcore/droidfs/EncryptedFileProvider$openFile$1.java sushi/hardcore/droidfs/EncryptedFileProvider.java sushi/hardcore/droidfs/VolumeDatabase.java sushi/hardcore/droidfs/content_providers/TemporaryFileProvider.java sushi/hardcore/droidfs/content_providers/VolumeProvider.java sushi/hardcore/droidfs/file_operations/FileOperationService.java sushi/hardcore/droidfs/file_viewers/MediaPlayer.java sushi/hardcore/droidfs/file_viewers/PdfViewer.java sushi/hardcore/droidfs/filesystems/GocryptfsVolume.java sushi/hardcore/droidfs/util/Wiper.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/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java
3	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	app/grapheneos/pdfviewer/PdfViewer$Channel$$ExternalSyntheticLambda1.java sushi/hardcore/droidfs/CameraActivity.java sushi/hardcore/droidfs/file_viewers/MediaPlayer.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	sushi/hardcore/droidfs/util/Wiper.java
5	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	sushi/hardcore/droidfs/VolumeDatabase.java
6	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	sushi/hardcore/droidfs/file_viewers/PdfViewer.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	arm64-v8a/libmux.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/libgocryptfs_jni.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
3	arm64-v8a/libcryfs_jni.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: ['__vsprintf_chk', '__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libavformat.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.	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.	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
5	arm64-v8a/libavutil.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.	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.	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
6	arm64-v8a/libmemfile.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.	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.	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	arm64-v8a/libgocryptfs.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.	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.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libavcodec.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.	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.	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	arm64-v8a/libimage_processing_util_jni.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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libmux.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
11	arm64-v8a/libgocryptfs_jni.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	arm64-v8a/libcryfs_jni.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: ['__vsprintf_chk', '__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libavformat.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.	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.	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/libavutil.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.	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.	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
15	arm64-v8a/libmemfile.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.	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.	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/libgocryptfs.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.	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.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libavcodec.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.	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.	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
18	arm64-v8a/libimage_processing_util_jni.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']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	app/grapheneos/pdfviewer/PdfViewer$$ExternalSyntheticLambda1.java
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/disklrucache/StrictLineReader.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/util/pool/FactoryPools.java sushi/hardcore/droidfs/EncryptedFileProvider$openFile$1.java sushi/hardcore/droidfs/EncryptedFileProvider.java sushi/hardcore/droidfs/adapters/VolumeAdapter.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	sushi/hardcore/droidfs/add_volume/SelectPathFragment.java
00104	Check if the given path is directory	file	sushi/hardcore/droidfs/MainActivity.java sushi/hardcore/droidfs/add_volume/SelectPathFragment.java
00036	Get resource file from res/raw directory	reflection	com/bumptech/glide/load/model/AssetUriLoader.java sushi/hardcore/droidfs/add_volume/SelectPathFragment.java
00125	Check if the given file path exist	file	sushi/hardcore/droidfs/MainActivity.java sushi/hardcore/droidfs/add_volume/CreateVolumeFragment.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00091	Retrieve data from broadcast	collection	sushi/hardcore/droidfs/SettingsActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory	file command	sushi/hardcore/droidfs/add_volume/CreateVolumeFragment.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO
Other Common Permissions	1/44	android.permission.FOREGROUND_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

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"key_permanently_invalidated_exception" : "KeyPermanentlyInvalidatedException"
"password" : "Senha"
"password" : "Contraseña"
"password" : "Пароль"
"password" : "Şifre"
"unrecoverable_key_exception" : "UnrecoverableKeyException"
"key_permanently_invalidated_exception_msg" : "□□□□□□□□□□□□□□□□□□□□□□"
"password" : "Password"
"password" : "□□"
"password" : "Passwort"

POSSIBLE SECRETS
"password" : "סיסמא"

SCAN LOGS

Timestamp	Event	Error
2025-08-01 01:21:43	Generating Hashes	OK
2025-08-01 01:21:43	Extracting APK	OK
2025-08-01 01:21:43	Unzipping	OK
2025-08-01 01:21:44	Parsing APK with androguard	OK
2025-08-01 01:21:46	Extracting APK features using aapt/aapt2	OK
2025-08-01 01:21:46	Getting Hardcoded Certificates/Keystores	OK
2025-08-01 01:21:53	Parsing AndroidManifest.xml	OK
2025-08-01 01:21:53	Extracting Manifest Data	OK

2025-08-01 01:21:54	Manifest Analysis Started	OK
2025-08-01 01:21:54	Performing Static Analysis on: DroidFS (sushi.hardcore.droidfs)	OK
2025-08-01 01:21:54	Fetching Details from Play Store: sushi.hardcore.droidfs	OK
2025-08-01 01:21:55	Checking for Malware Permissions	OK
2025-08-01 01:21:55	Fetching icon path	OK
2025-08-01 01:21:55	Library Binary Analysis Started	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libmux.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libgocryptfs_jni.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libcryfs_jni.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libavformat.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libavutil.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libmemfile.so	OK

2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libgocryptfs.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libavcodec.so	OK
2025-08-01 01:21:55	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libmux.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libgocryptfs_jni.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libcryfs_jni.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libavformat.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libavutil.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libmemfile.so	OK
2025-08-01 01:21:55	Analyzing lib/arm64-v8a/libgocryptfs.so	OK
2025-08-01 01:21:56	Analyzing lib/arm64-v8a/libavcodec.so	OK
2025-08-01 01:21:56	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK

2025-08-01 01:21:56	Reading Code Signing Certificate	OK
2025-08-01 01:21:58	Running APKiD 2.1.5	OK
2025-08-01 01:22:01	Detecting Trackers	OK
2025-08-01 01:22:03	Decompiling APK to Java with JADX	OK
2025-08-01 01:23:03	Converting DEX to Smali	OK
2025-08-01 01:23:03	Code Analysis Started on - java_source	OK
2025-08-01 01:23:04	Android SBOM Analysis Completed	OK
2025-08-01 01:23:13	Android SAST Completed	OK
2025-08-01 01:23:13	Android API Analysis Started	OK
2025-08-01 01:23:19	Android API Analysis Completed	OK
2025-08-01 01:23:20	Android Permission Mapping Started	OK
2025-08-01 01:23:22	Android Permission Mapping Completed	OK

2025-08-01 01:23:23	Android Behaviour Analysis Started	OK
2025-08-01 01:23:29	Android Behaviour Analysis Completed	OK
2025-08-01 01:23:29	Extracting Emails and URLs from Source Code	OK
2025-08-01 01:23:31	Email and URL Extraction Completed	OK
2025-08-01 01:23:31	Extracting String data from APK	OK
2025-08-01 01:23:32	Extracting String data from SO	OK
2025-08-01 01:23:32	Extracting String data from Code	OK
2025-08-01 01:23:32	Extracting String values and entropies from Code	OK
2025-08-01 01:23:34	Performing Malware check on extracted domains	OK
2025-08-01 01:23:36	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.