ANDROID STATIC ANALYSIS REPORT

File Name:	testsf.apk
Package Name:	site.realanime.animlov.animlov
Scan Date:	Oct. 9, 2025, 6:46 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	11	0	0	1

FILE INFORMATION

File Name: testsf.apk
Size: 4.86MB
MD5: eed695e95b019c2e0cd575725117f11c
SHA1: d1ea91eab466d1433ea21bb6f6fd4426c2f4e8cf
SHA256: abb882a555e3b0d298b4560c354dcded84d7850c0611275fec6315e9026fd50d

APP INFORMATION

App Name: AnimLovers
Package Name: site.realanime.animlov.animlov
Main Activity: site.realanime.animlov.animlov.Splash
Target SDK: 27
Min SDK: 21
Max SDK:
Android Version Name: 1.8
Android Version Code: 8

APP COMPONENTS

Activities: 16
Services: 9
Receivers: 4
Providers: 1
Exported Activities: 2
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=ID, ST=Sumatera Utara, L=Medan, O=RA, OU=RA, CN=M arief
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-10-10 10:23:23+00:00
Valid To: 2043-10-04 10:23:23+00:00
Issuer: C=ID, ST=Sumatera Utara, L=Medan, O=RA, OU=RA, CN=M arief
Serial Number: 0x1e7c474b
Hash Algorithm: sha256
md5: 6ccc9f008fdcb1fd2a6f731ca83ba34f
sha1: c6e83d332a2b0aa315b3386ea7890232d551fd6f
sha256: 6ea294784a14d272e89fbada78b695bf86a33b26724971cab8945e66fbf9716a
sha512: 6432d75678371441ff70cc90a231aed7f2bd7ad619c0e6d100fb002fd9625aed5391539a4176381fc56be5f57fe0d704fb370b935002e6a7fea59688a571a0fa
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
			Access fine location sources, such as the Global Positioning System on the phone, where available.

android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check possible ro.secure check emulator file check FINDINGS: Compiler DETAILS: r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | 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	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.
3	Activity (site.realanime.animlov.animlov.PmMe.InboxView) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Broadcast Receiver (com.startapp.android.publish.common.metaData.BootCompleteListener) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
5	Service (site.realanime.animlov.animlov.Service.MyFirebaseMessagingService) is not Protected.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other

	An intent-filter exists.		application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
6	Service (com.google.firebase.messaging.FirebaseMessagingService) 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.
7	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [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. 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.
8	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
9	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.

10	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	4/45	android.permission.CHANGE_WIFI_STATE, android.permission.BLUETOOTH, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

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
animlov-fcea5.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://animlov-fcea5.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://animlov-fcea5.firebaseio.com"
"google_api_key" : "AIzaSyBvQp2eV-b7LNs6fayF1F6_NSVC0McMhCA"
"google_crash_reporting_api_key" : "AIzaSyBvQp2eV-b7LNs6fayF1F6_NSVC0McMhCA"

SCAN LOGS

Timestamp	Event	Error
2025-10-09 06:46:35	Generating Hashes	OK
2025-10-09 06:46:35	Extracting APK	OK
2025-10-09 06:46:35	Unzipping	OK
2025-10-09 06:46:35	Getting Hardcoded Certificates/Keystores	OK
2025-10-09 06:46:41	Parsing AndroidManifest.xml	OK
2025-10-09 06:46:41	Parsing APK with androguard	OK
2025-10-09 06:46:41	Extracting Manifest Data	OK
2025-10-09 06:46:41	Performing Static Analysis on: AnimLovers (site.realanime.animlov.animlov)	OK
2025-10-09 06:46:41	Fetching Details from Play Store: site.realanime.animlov.animlov	OK
2025-10-09 06:46:42	Manifest Analysis Started	OK
2025-10-09 06:46:42	Checking for Malware Permissions	OK

2025-10-09 06:46:42	Fetching icon path	OK
2025-10-09 06:46:42	Library Binary Analysis Started	OK
2025-10-09 06:46:42	Reading Code Signing Certificate	OK
2025-10-09 06:46:43	Running APKiD 2.1.5	OK
2025-10-09 06:46:53	Detecting Trackers	OK
2025-10-09 06:46:55	Decompiling APK to Java with jadx	OK
2025-10-09 06:46:55	Converting DEX to Smali	OK
2025-10-09 06:46:55	Code Analysis Started on - java_source	OK
2025-10-09 06:46:55	Android SAST Completed	OK
2025-10-09 06:46:55	Android API Analysis Started	OK
2025-10-09 06:46:56	Android Permission Mapping Started	OK

2025-10-09 06:46:56	Android Permission Mapping Completed	OK
2025-10-09 06:46:56	Finished Code Analysis, Email and URL Extraction	OK
2025-10-09 06:46:56	Extracting String data from APK	OK
2025-10-09 06:46:56	Extracting String data from Code	OK
2025-10-09 06:46:56	Extracting String values and entropies from Code	OK
2025-10-09 06:46:56	Performing Malware check on extracted domains	OK
2025-10-09 06:47:00	Saving to Database	OK