ANDROID STATIC ANALYSIS REPORT

Testdroid (0.3)

File Name:	testdroid-sample-app.apk
Package Name:	com.testdroid.sample.android
Scan Date:	April 19, 2025, 11:02 a.m.
App Security Score:	24/100 (CRITICAL RISK)
Grade:	F

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
6	2	1	1	1

FILE INFORMATION

File Name: testdroid-sample-app.apk
Size: 1.35MB
MD5: 039206d422cf01b82d82305734d7076b
SHA1: 92ff6878d7b11030fd7c8cf74ecf97f1ed47f310
SHA256: d156ecae769ad9698f2946d5e05422cf0bff7ca3a01756235dbfdc96a3161be1

APP INFORMATION

App Name: Testdroid
Package Name: com.testdroid.sample.android
Main Activity: com.testdroid.sample.android.MM_MainMenu
Target SDK: 19
Min SDK: 14
Max SDK:
Android Version Name: 0.3
Android Version Code: 1

APP COMPONENTS

Activities: 11
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-10-16 18:20:33+00:00
Valid To: 2042-10-09 18:20:33+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x1e0bf523
Hash Algorithm: sha256
md5: 4564ad2969f13129b04b2e288fe1c7ee
sha1: 12a050a949e10f12b0af48ed64da8cbf0f9a9b1c
sha256: e9958eeed351ff39389b253dbe9a066c10afaf32d2adf90716054c4f59eac904
sha512: e3712a817a70c3d925a3ad348e1a73d502eba134adb4aba0dce7e41a036984924f232db9c0c08bba926e525d0450256953577c219c5d1f19407e0cd8c8804b42
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_MOCK_LOCATION	dangerous	mock location sources for testing	Create mock location sources for testing. Malicious applications can use this to override the location and/or status returned by real-location sources such as GPS or Network providers.
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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

<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.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0-4.0.2, [minSdk=14]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
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.

CODE ANALYSIS

HIGH: **2** | WARNING: **1** | 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	com/testdroid/sample/android/DI_DeviceInfo.java com/testdroid/sample/android/ES_ExternalStorage.java com/testdroid/sample/android/FC_Functions.java com/testdroid/sample/android/HY_Hybrid.java com/testdroid/sample/android/PT_PingTest.java
2	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/testdroid/sample/android/HY_Hybrid.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/testdroid/sample/android/DI_DeviceInfo.java
4	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/testdroid/sample/android/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/testdroid/sample/android/ES_ExternalStorage.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	1/44	android.permission.ACCESS_MOCK_LOCATION

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
www.google.com	ok	**IP:** 142.250.183.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

SCAN LOGS

Timestamp	Event	Error
2025-04-19 11:02:04	Generating Hashes	OK
2025-04-19 11:02:04	Extracting APK	OK
2025-04-19 11:02:04	Unzipping	OK

2025-04-19 11:02:05	Parsing APK with androguard	OK
2025-04-19 11:02:05	Extracting APK features using aapt/aapt2	OK
2025-04-19 11:02:05	Getting Hardcoded Certificates/Keystores	OK
2025-04-19 11:02:07	Parsing AndroidManifest.xml	OK
2025-04-19 11:02:07	Extracting Manifest Data	OK
2025-04-19 11:02:07	Manifest Analysis Started	OK
2025-04-19 11:02:07	Performing Static Analysis on: Testdroid (com.testdroid.sample.android)	OK
2025-04-19 11:02:07	Fetching Details from Play Store: com.testdroid.sample.android	OK
2025-04-19 11:02:08	Checking for Malware Permissions	OK
2025-04-19 11:02:08	Fetching icon path	OK

2025-04-19 11:02:08	Library Binary Analysis Started	OK
2025-04-19 11:02:08	Reading Code Signing Certificate	OK
2025-04-19 11:02:08	Running APKiD 2.1.5	OK
2025-04-19 11:02:10	Detecting Trackers	OK
2025-04-19 11:02:10	Decompiling APK to Java with JADX	OK
2025-04-19 11:02:14	Converting DEX to Smali	OK
2025-04-19 11:02:14	Code Analysis Started on - java_source	OK
2025-04-19 11:02:15	Android SBOM Analysis Completed	OK
2025-04-19 11:02:15	Android SAST Completed	OK
2025-04-19 11:02:15	Android API Analysis Started	OK
2025-04-19 11:02:15	Android API Analysis Completed	OK

2025-04-19 11:02:16	Android Permission Mapping Started	OK
2025-04-19 11:02:16	Android Permission Mapping Completed	OK
2025-04-19 11:02:16	Android Behaviour Analysis Started	OK
2025-04-19 11:02:17	Android Behaviour Analysis Completed	OK
2025-04-19 11:02:17	Extracting Emails and URLs from Source Code	OK
2025-04-19 11:02:17	Email and URL Extraction Completed	OK
2025-04-19 11:02:17	Extracting String data from APK	OK
2025-04-19 11:02:17	Extracting String data from Code	OK
2025-04-19 11:02:17	Extracting String values and entropies from Code	OK
2025-04-19 11:02:17	Performing Malware check on extracted domains	OK
2025-04-19 11:02:18	Saving to Database	OK

Report Generated by - MobSF v4.3.2

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.

iSec
SERVICES PVT.LTD.
Securing the InSecure