MOBSF

ANDROID STATIC ANALYSIS REPORT

V Hospice (1.0.0)

File Name:	app-debug.apk
Package Name:	ru.iteco.fmhandroid
Scan Date:	June 16, 2025, 3:42 a.m.
App Security Score:	24/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	2	0	1	0

FILE INFORMATION

File Name: app-debug.apk
Size: 9.67MB
MD5: 30319562bcb44eca13fbf4a3968e9853
SHA1: c6af75b644e11cee40658c02540097505841df9b
SHA256: 34fc0a8e03115198527e9031cd4a25147d018392be3dc71bff4443426db3979f

APP INFORMATION

App Name: V Hospice
Package Name: ru.iteco.fmhandroid
Main Activity: ru.iteco.fmhandroid.ui.AppActivity
Target SDK: 32
Min SDK: 21
Max SDK:
Android Version Name: 1.0.0

Android Version Code: 14

APP COMPONENTS

Activities: 1
Services: 6
Receivers: 2
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: None
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-03-30 19:32:20+00:00
Valid To: 2052-03-22 19:32:20+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: ba326ea5d87a9226f66ca55f72ee56f8
sha1: 2c1aa19ef5140fde59d64d9dff39133e46f4310f
sha256: fb0009366d612fbc9c4199df6504784d9cd0d24c9551e6a6b3d7cec36805cd09
sha512: 997cb9d0427b945f4fcc5b939aa46f66f70eccff5cbb0b27b7b4c68caa626bd587c296dfacb0d782bbceacd87507fcbe4275e7ecd9320991b28fa303a904d351
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5b3a5f28ddb35719f9d9d65ac98f9d48781c7fe309b1a0a9924e7b04040ee4dd
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

APKID ANALYSIS

FILE	DETAILS
classes8.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

FILE	DETAILS
classes14.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)
classes13.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)
classes10.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes11.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes6.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)
classes5.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)
classes12.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)
classes2.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Compiler: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes15.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</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
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

TITLE	SEVERITY	DESCRIPTION
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **4** | WARNING: **0** | 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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Application is in Test Mode [android:testOnly=true]	high	It may expose functionality or data outside of itself that would cause a security hole.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/729587742060/namespaces/firebase:fetch?key=AIzaSyCU9yOr300iTEudvLNPSI-NUlql-KrS1SU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
vhospice.org	ok	**IP:** 89.106.171.126 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"authorization" : "Authorization"
"google_api_key" : "AIzaSyCU9yOr300iTEudvLNPSI-NUlql-KrS1SU"
"google_crash_reporting_api_key" : "AIzaSyCU9yOr300iTEudvLNPSI-NUlql-KrS1SU"
"password" : "Password"
"authorization" : "Авторизация"
"password" : "Пароль"

SCAN LOGS

Timestamp	Event	Error
2025-06-16 03:42:24	Generating Hashes	OK

2025-06-16 03:42:24	Extracting APK	OK
2025-06-16 03:42:24	Unzipping	OK
2025-06-16 03:42:24	Parsing APK with androguard	OK
2025-06-16 03:42:25	Extracting APK features using aapt/aapt2	OK
2025-06-16 03:42:25	Getting Hardcoded Certificates/Keystores	OK
2025-06-16 03:42:28	Parsing AndroidManifest.xml	OK
2025-06-16 03:42:28	Extracting Manifest Data	OK
2025-06-16 03:42:28	Manifest Analysis Started	OK
2025-06-16 03:42:28	Performing Static Analysis on: V Hospice (ru.iteco.fmhandroid)	OK
2025-06-16 03:42:28	Fetching Details from Play Store: ru.iteco.fmhandroid	OK

2025-06-16 03:42:28	Checking for Malware Permissions	OK
2025-06-16 03:42:28	Fetching icon path	OK
2025-06-16 03:42:28	Library Binary Analysis Started	OK
2025-06-16 03:42:28	Reading Code Signing Certificate	OK
2025-06-16 03:42:29	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/30319562bcb44eca13fbf4a3968e9853/30319562bcb44eca13fbf4a3968e9853.apk'])
2025-06-16 03:42:29	Running APKiD 2.1.5	OK
2025-06-16 03:42:30	Detecting Trackers	OK
2025-06-16 03:42:37	Decompiling APK to Java with JADX	OK
2025-06-16 03:42:38	Decompiling with JADX failed	Exception('Executable/Library Tampering Detected')
2025-06-16 03:42:38	Converting DEX to Smali	OK

2025-06-16 03:42:38	Code Analysis Started on - java_source	OK
2025-06-16 03:42:42	Android SBOM Analysis Completed	OK
2025-06-16 03:42:44	Android SAST Completed	OK
2025-06-16 03:42:44	Android API Analysis Started	OK
2025-06-16 03:42:45	Android API Analysis Completed	OK
2025-06-16 03:42:46	Android Permission Mapping Started	OK
2025-06-16 03:42:47	Android Permission Mapping Completed	OK
2025-06-16 03:42:47	Android Behaviour Analysis Started	OK
2025-06-16 03:42:48	Android Behaviour Analysis Completed	OK
2025-06-16 03:42:48	Extracting Emails and URLs from Source Code	OK

2025-06-16 03:42:48	Email and URL Extraction Completed	OK
2025-06-16 03:42:48	Extracting String data from APK	OK
2025-06-16 03:42:48	Extracting String data from Code	OK
2025-06-16 03:42:48	Extracting String values and entropies from Code	OK
2025-06-16 03:42:48	Performing Malware check on extracted domains	OK
2025-06-16 03:42:50	Saving to Database	OK

Report Generated by - MobSF v4.3.3

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.