



# ANDROID STATIC ANALYSIS REPORT



 Mach3Pendant  
(@string/version)

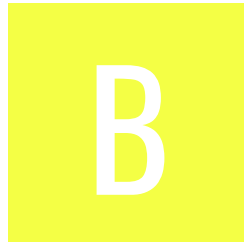
File Name: installer338.apk

Package Name: gr.ratmole.android.Mach3Pendant






Scan Date: May 31, 2022, 8:36 a.m.

App Security Score: 53/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	4	1	1	1

## FILE INFORMATION

File Name: installer338.apk

Size: 0.75MB

MD5: 568f4ee7b108874da47c8d3143a6674d

SHA1: eff6abe8bd3eed31e6535e179dec39a5fdf5dd53

SHA256: f0ce9fcc90b664b3503d08fb2e8b62ae45b2c366b6cf20ba3b5badacb89157c5

## APP INFORMATION

App Name: Mach3Pendant

Package Name: gr.ratmole.android.Mach3Pendant

Main Activity: gr.ratmole.android.Mach3Pendant.Mach3PendantActivity

Target SDK: 14

Min SDK: 14

Max SDK:

Android Version Name: @string/version

Android Version Code: 14

## APP COMPONENTS

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

## CERTIFICATE INFORMATION

APK is signed  
v1 signature: True  
v2 signature: False  
v3 signature: False  
Found 1 unique certificates  
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid  
Signature Algorithm: rsassa\_pkcs1v15  
Valid From: 2016-10-13 21:41:44+00:00  
Valid To: 2044-02-29 21:41:44+00:00  
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid  
Serial Number: 0x64f4cd4a  
Hash Algorithm: sha256  
md5: a9c1f6e699575f421224d50129e1a186  
sha1: 8e16f485a5baa44d712b82d302c6bab6b56dcdce  
sha256: 7521abc282fd79c30a68dd79b110cc600ac5e317780e6b2049ae5458cfb36263  
sha512: c6ef7b661b6d40d869d55b6c9cb4c5fd69a435c63630065b56a006ea0a05c1dc33b5989b612da0280384ebfdbf79bdb1915a86cc8adf1fc67e0f882dc519691b

TITLE	SEVERITY	DESCRIPTION
Signed Application	<a href="#">info</a>	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 PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.

## 🔍 APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	dx (possible dexmerge)
	Manipulator Found	dexmerge

## NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

## CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/esotericsoftware/kryo/util/ObjectMap.java com/esotericsoftware/kryonet/util/ObjectIntMap.java com/esotericsoftware/jsonbeans/ObjectMap.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	gr/ratmole/android/Mach3Pendant/model/Key.java com/esotericsoftware/kryonet/Connection.java com/esotericsoftware/kryo/util/Util.java gr/ratmole/android/Mach3Pendant/Utils/Log.java gr/ratmole/android/Mach3Pendant/fragments/OSLevelController.java gr/ratmole/android/Mach3Pendant/model/HotKeys.java gr/ratmole/android/Mach3Pendant/Mach3PendantActivity.java com/esotericsoftware/kryonet/Listener.java com/esotericsoftware/kryonet/Server.java gr/ratmole/android/Mach3Pendant/ConnectionController.java com/esotericsoftware/kryonet/TcpConnection.java com/esotericsoftware/jsonbeans/JsonReader.java com/esotericsoftware/kryonet/rmi/ObjectSpace.java com/esotericsoftware/kryonet/Client.java gr/ratmole/android/Mach3Pendant/ConnectivityManager.java com/esotericsoftware/kryonet/UdpConnection.java gr/ratmole/android/Mach3Pendant/Utils/HotKeysHandler.java com/esotericsoftware/kryonet/JsonSerialization.java com/esotericsoftware/minlog/Log.java com/esotericsoftware/kryo/Kryo.java
3	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	gr/ratmole/android/Mach3Pendant/model/HotKeys.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	gr/ratmole/android/Mach3Pendant/shared/ServerGreeting.java

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	<a href="#">FCS_RBG_EXT.1.1</a>	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	<a href="#">FCS_STO_EXT.1.1</a>	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	<a href="#">FCS_CKM_EXT.1.1</a>	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	<a href="#">FDP_DEC_EXT.1.1</a>	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	<a href="#">FDP_DEC_EXT.1.2</a>	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	<a href="#">FDP_NET_EXT.1.1</a>	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	<a href="#">FDP_DAR_EXT.1.1</a>	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.



NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: <a href="#">Google Map</a>
schemas.android.com	ok	No Geolocation information available.

### Report Generated by - MobSF v3.5.2 Beta

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.