

## ANDROID STATIC ANALYSIS REPORT



Yucata Envoy (0.5.3)

File Name:	installer3806.apk
Package Name:	kaba.yucata.envoy
Scan Date:	May 31, 2022, 6:25 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

### FINDINGS SEVERITY

<del>派</del> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	≪ HOTSPOT
1	4	1	1	0

#### FILE INFORMATION

File Name: installer3806.apk

Size: 1.79MB

MD5: 9b59b5fc23359655826f809045ef8ea4

SHA1: 8f5f72631c39e21fead49589ef3fb32108867c67

SHA256: 6040f9751d6fb58789d47f63f35df1bd9f556a5f2060639f4d49f079536f666f

## **i** APP INFORMATION

App Name: Yucata Envoy

Package Name: kaba.yucata.envoy

Main Activity: kaba.yucata.envoy.GameCountActivity

Target SDK: 28 Min SDK: 15 Max SDK:

Android Version Name: 0.5.3
Android Version Code: 503

#### **EE** APP COMPONENTS

Activities: 5 Services: 1 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2017-10-18 15:26:59+00:00 Valid To: 2045-03-05 15:26:59+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x71795d9a Hash Algorithm: sha256

md5: 961b406ffaebf8872565c55e9bd145b8

sha1: 8e380d050ca033617c9cba3d083183b7185a85c5

sha256: b3f2d56180b8b1691e9af67ed930bb1e01a58ff5cf7fe8d436e6809cdc5e9663

sha512: ce88fceee49e2c1a013ab537023f5c77220beafe84dc18315cb745943034c115862b2572580bcae14a57a8d506231c0dbbfb899b1bed5e7d79476dc9cdd47224

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 PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

## **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	r8	

## **△** NETWORK SECURITY

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

## **Q** MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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

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	kaba/yucata/envoy/datalink/Lo aderTask.java kaba/yucata/envoy/service/Ba sicDataService.java kaba/yucata/envoy/service/Loll iJobService.java kaba/yucata/envoy/service/Loll iDataService.java kaba/yucata/envoy/datalink/St ateInfo.java kaba/yucata/envoy/service/Dat aService.java kaba/yucata/envoy/SettingsFra gment.java
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	kaba/yucata/envoy/PrefsHelpe r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	kaba/yucata/envoy/datalink/G amelistDbHelper.java

## ■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	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
7	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.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

## **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
www.gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map
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: Google Map

DOMAIN	STATUS	GEOLOCATION
www.yucata.de	ok	IP: 172.67.75.24  Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

### **▶** HARDCODED SECRETS

# POSSIBLE SECRETS "k\_pref\_password": "secret" "k\_pref\_username": "username"

#### 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.