



ANDROID STATIC ANALYSIS REPORT



 FlixOnline (1.2)

File Name: 1d097436927f85b1ab9bf69913071abd0845bfcf1afa186112e91e1ca22e32df.apk

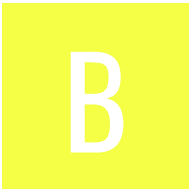
Package Name: com.fab.wflixonline

Scan Date: April 26, 2025, 8:15 p.m.

App Security Score:

46/100 (MEDIUM RISK)

Grade:



 FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	5	1	1	1

 FILE INFORMATION

File Name: 1d097436927f85b1ab9bf69913071abd0845bfcf1afa186112e91e1ca22e32df.apk
Size: 1.28MB
MD5: 7229dc5304cc5f9f5ec4e2af25512c53
SHA1: 14e8ef9731417bc562ff46d1b09b2fc66fb65b51
SHA256: 1d097436927f85b1ab9bf69913071abd0845bfcf1afa186112e91e1ca22e32df

APP INFORMATION

App Name: FlixOnline
Package Name: com.fab.wflixonline
Main Activity: com.fab.wflixonline.MainActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 1.2
Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 3
Receivers: 2
Providers: 0
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-08 14:03:41+00:00
Valid To: 2050-12-08 14:03:41+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xa5840901fe4806fe964680d987e057d4346e8af1
Hash Algorithm: sha256
md5: 741338567fed26fca3a233f9ecd1a61f
sha1: bec2c0448558729c1edf4e45ab76b6a3ee6e42b7
sha256: 8853ea6d89125f88db9c34ac93775f93672e1fa342cf48e0637a20b05f29ac42

sha512: bbecaea86338846af917be9b23ca5d44abba9df4ab1010ef49ba355e01c9b4729002f66e20e1eb19ebb653b2770caef1b8599670a84b39b5a7cb4ee165cf3cb9
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3ca0cf3ff1fad5db775e2f87fe6a05f85424fccd7a28afe79e269f9ce80f7d0b
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

🌀 APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	r8

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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	Service (com.fab.wflixonline.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [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. 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.
4	Broadcast Receiver (com.fab.wflixonline.DeviceBootReceiver) is not Protected. [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.

</> CODE ANALYSIS

HIGH: 0 | 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	a/b/k/f.java a/b/p/c.java a/b/p/e/d.java a/b/p/e/f.java a/b/q/a0.java a/b/q/e0.java a/b/q/f0.java a/b/q/j0.java a/b/q/m0.java a/b/q/o.java a/b/q/p0.java a/b/q/r.java a/b/q/x.java a/b/q/z.java a/e/f/c.java a/e/f/d.java a/e/f/e.java a/e/f/f.java a/e/f/g.java a/e/h/b.java a/e/k/a.java a/e/l/a.java a/e/l/b.java a/e/l/e.java a/e/l/n.java a/e/l/s.java a/f/a/b.java a/h/a/a.java a/i/d/a.java a/i/d/d.java a/i/d/o.java a/i/d/q.java a/i/d/u.java a/i/d/w.java a/o/a/a/f.java b/a/a/a/a.java b/a/b/d.java b/a/b/j.java b/a/b/n.java b/a/b/u/b.java b/a/b/u/d.java b/b/a/b.java b/b/a/h.java b/b/a/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/b/a/k/a.java b/b/a/l/d.java b/b/a/l/e.java b/b/a/m/t/b.java b/b/a/m/t/j.java b/b/a/m/t/l.java b/b/a/m/t/p/b.java b/b/a/m/u/b0.java b/b/a/m/u/c0/i.java b/b/a/m/u/c0/j.java b/b/a/m/u/d0/e.java b/b/a/m/u/d0/j.java b/b/a/m/u/e0/a.java b/b/a/m/u/i.java b/b/a/m/u/j.java b/b/a/m/u/l.java b/b/a/m/u/r.java b/b/a/m/v/c.java b/b/a/m/v/d.java b/b/a/m/v/f.java b/b/a/m/v/s.java b/b/a/m/v/t.java b/b/a/m/w/a.java b/b/a/m/w/c/b0.java b/b/a/m/w/c/c.java b/b/a/m/w/c/k.java b/b/a/m/w/c/m.java b/b/a/m/w/c/n.java b/b/a/m/w/c/r.java b/b/a/m/w/c/z.java b/b/a/m/w/g/a.java b/b/a/m/w/g/d.java b/b/a/m/w/g/j.java b/b/a/n/e.java b/b/a/n/k.java b/b/a/n/l.java b/b/a/n/o.java b/b/a/q/g.java b/b/a/q/h/i.java b/b/a/s/k/a.java b/c/a/a.java com/fab/wflixonline/NotificationService.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	b/b/a/m/u/q.java

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b/a/b/d.java b/a/b/u/d.java
00013	Read file and put it into a stream	file	a/b/k/f.java a/e/f/e.java a/e/f/f.java b/a/b/d.java b/b/a/k/a.java b/b/a/m/h.java b/b/a/m/j.java b/b/a/m/v/f.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/fab/wflixonline/MainActivity.java com/fab/wflixonline/TheJobChromium.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/fab/wflixonline/MainActivity.java com/fab/wflixonline/TheJobChromium.java
00191	Get messages in the SMS inbox	sms	a/b/q/e0.java
00036	Get resource file from res/raw directory	reflection	a/b/q/e0.java
00096	Connect to a URL and set request method	command network	b/a/b/u/f.java
00089	Connect to a URL and receive input stream from the server	command network	b/a/b/u/f.java b/b/a/m/t/j.java
00109	Connect to a URL and get the response code	network command	b/a/b/u/f.java b/b/a/m/t/j.java
00030	Connect to the remote server through the given URL	network	b/b/a/m/t/j.java
00012	Read data and put it into a buffer stream	file	b/a/b/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/fab/wflixonline/MainActivity.java
00024	Write file after Base64 decoding	reflection file	a/b/k/f.java
00077	Read sensitive data(SMS, CALLOG, etc)	collection sms callog calendar	b/b/a/m/t/p/b.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	1/44	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
netflixwatch.site	malware URL: netflixwatch.site IP: N/A Description: Malicious Domain tagged by Maltrail	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
flixxonline.site	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
i.imgur.com	ok	IP: 199.232.192.193 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"state_api" : "https://netflixwatch.site/settings.php"

SCAN LOGS

Timestamp	Event	Error
2025-04-26 20:15:03	Generating Hashes	OK
2025-04-26 20:15:03	Extracting APK	OK
2025-04-26 20:15:03	Unzipping	OK
2025-04-26 20:15:03	Parsing APK with androguard	OK

2025-04-26 20:15:03	Extracting APK features using aapt/aapt2	OK
2025-04-26 20:15:03	Getting Hardcoded Certificates/Keystores	OK
2025-04-26 20:15:04	Parsing AndroidManifest.xml	OK
2025-04-26 20:15:04	Extracting Manifest Data	OK
2025-04-26 20:15:04	Manifest Analysis Started	OK
2025-04-26 20:15:04	Performing Static Analysis on: FlixOnline (com.fab.wflixonline)	OK
2025-04-26 20:15:04	Fetching Details from Play Store: com.fab.wflixonline	OK
2025-04-26 20:15:05	Checking for Malware Permissions	OK
2025-04-26 20:15:05	Fetching icon path	OK
2025-04-26 20:15:05	Library Binary Analysis Started	OK
2025-04-26 20:15:05	Reading Code Signing Certificate	OK
2025-04-26 20:15:05	Running APKID 2.1.5	OK
2025-04-26 20:15:06	Updating Trackers Database....	OK
2025-04-26 20:15:06	Detecting Trackers	OK

2025-04-26 20:15:06	Decompiling APK to Java with JADX	OK
2025-04-26 20:15:08	Converting DEX to Smali	OK
2025-04-26 20:15:08	Code Analysis Started on - java_source	OK
2025-04-26 20:15:09	Android SBOM Analysis Completed	OK
2025-04-26 20:15:09	Android SAST Completed	OK
2025-04-26 20:15:09	Android API Analysis Started	OK
2025-04-26 20:15:09	Android API Analysis Completed	OK
2025-04-26 20:15:10	Android Permission Mapping Started	OK
2025-04-26 20:15:10	Android Permission Mapping Completed	OK
2025-04-26 20:15:10	Android Behaviour Analysis Started	OK
2025-04-26 20:15:11	Android Behaviour Analysis Completed	OK
2025-04-26 20:15:11	Extracting Emails and URLs from Source Code	OK
2025-04-26 20:15:11	Email and URL Extraction Completed	OK
2025-04-26 20:15:11	Extracting String data from APK	OK

2025-04-26 20:15:11	Extracting String data from Code	OK
2025-04-26 20:15:11	Extracting String values and entropies from Code	OK
2025-04-26 20:15:11	Performing Malware check on extracted domains	OK
2025-04-26 20:15:12	Saving to Database	OK
2025-04-26 20:21:55	Performing Malware check on extracted domains	OK
2025-04-26 20:21:56	Detecting Trackers from Domains	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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).