MOBSF

ANDROID STATIC ANALYSIS REPORT

JustFit (1.5.5)

File Name:	fitness.home.workout.weight.loss_155.apk
Package Name:	fitness.home.workout.weight.loss
Scan Date:	Sept. 1, 2025, 1:17 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	16	2	3	1

FILE INFORMATION

File Name: fitness.home.workout.weight.loss_155.apk
Size: 37.49MB
MD5: 7362c64a4d235606706bb46185a6e1a0
SHA1: bcfa18a24b97d907f792d65f5d3985a38abd925f
SHA256: 08c8f7cf30ab8cf1f9be6e8626be8b284e6535a98b8456c1d0f7f428f4dc2b4b

APP INFORMATION

App Name: JustFit
Package Name: fitness.home.workout.weight.loss
Main Activity: life.enerjoy.justfit.main.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.5.5

Android Version Code: 155

APP COMPONENTS

Activities: 15
Services: 10
Receivers: 7
Providers: 9
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=HK, ST=HK, L=HK, O=Enerjoy, OU=Business, CN=Enerjoy
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-03 11:30:44+00:00
Valid To: 2119-11-09 11:30:44+00:00
Issuer: C=HK, ST=HK, L=HK, O=Enerjoy, OU=Business, CN=Enerjoy
Serial Number: 0x7c3ff50e
Hash Algorithm: sha256
md5: 5ab6ca0dbd93aad4fe9651e4940a340e
sha1: bfbea2cfe1f3e9abc3780f4d747aa85efe316235
sha256: 5d962fa108314b9edf866adfc17bb1121ffad4be74bd7e1d14cd8e6776a7aa60
sha512: 8e63aa07d51fea918f12b1665654af82bcbfa8035807786ba7acc3fef44e4203ca328601a0af8924da1e5dd3d17d441f5008d65b5089e0e49c6369c5cbdad4f0
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 842e9a0f6515e97dc643c677f7d852386d84c8bbd7a4e2d8d40bdeb893be8019
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
fitness.home.workout.weight.loss.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
fitness.home.workout.weight.loss.permission.LE_FRAMEWORK	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
7362c64a4d235606706bb46185a6e1a0.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

FILE	DETAILS
classes.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>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu 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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
life.enerjoy.justfit.module.OneLinkActivity	Schemes: https://, Hosts: justfit-inapp-event.onelink.me,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.fitness.home.workout.weight.loss,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (life.enerjoy.justfit.module.OneLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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. 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.
6	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) 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.
7	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 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: **2** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A1/f.java B/C0009d.java B/P.java B/V.java C8/Q.java E4/b.java E4/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				E4/p.java E4/q.java E4/t.java E4/u.java E4/v.java E4/y.java F7/j.java G/c.java G4/c.java G7/a.java H4/c.java H4/d.java H7/a.java H7/c.java J4/b.java J6/B1.java J6/CallableC0323t0.java J6/L.java J6/R0.java J6/RunnableC0312n0.java J6/X.java J7/b.java K4/A.java K4/h.java K4/i.java K4/k.java K7/k.java K7/n.java K7/p.java K7/q.java K7/s.java K7/u.java K7/v.java L/e.java L4/f.java L4/g.java L6/a.java L7/g.java La/b.java Lb/d.java Lb/q.java

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	Le/b.java M2/b.java N4/c.java O1/T.java O2/k.java O4/A.java O4/C0487b.java O4/C0489d.java P7/b.java Q4/b.java Q7/c.java Qb/f.java R4/A.java R4/C0533b.java R4/C0534c.java R4/F.java R4/i.java R4/m.java R4/p.java R4/r.java R4/v.java Se/l.java Se/n.java Te/d.java U1/p.java Ua/d.java V4/a.java V4/i.java W/g.java X5/b.java Z4/g.java a5/C0797d.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/b.java com/bumptech/glide/k.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/k.java com/bumptech/glide/m.java com/bumptech/glide/manager/l.java com/bumptech/glide/manager/m.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/r.java f2/AbstractC1483c.java f6/c.java f6/h.java i7/e.java kc/C1890e.java kc/C1892g.java kc/C1893h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				life/enerjoy/justfit/module/ratealert/RateAlertFragment.java o5/k.java o6/i.java o7/d.java o7/f.java p1/C2249n.java p6/f.java p6/h.java q1/c.java r6/e.java r6/f.java s6/BinderC2494D.java s6/HandlerC2493C.java v1/f.java v7/a.java v7/c.java w8/c.java wb/C2862a.java x6/b.java xe/C2905b.java xe/C2907d.java xe/f.java y4/C2948b.java y4/C2949c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	I4/g.java Ja/c.java K4/d.java K4/r.java K4/y.java Mb/o.java Zb/c.java d1/C1331J.java g4/C1575b.java life/enerjoy/testsolution/room/entity/EtInfo.java life/enerjoy/testsolution/room/entity/NewGodEtInfo.java m0/C1974a0.java r2/C2416b.java
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	J6/H1.java Ua/d.java o5/k.java y4/C2948b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	B/C0009d.java B/P.java F2/b.java F7/b.java H0/C0200a.java H7/a.java J6/B0.java J6/B1.java J6/C0303k.java J6/J.java K3/b.java P2/l.java f6/c.java f6/f.java f6/h.java g6/j.java g6/k.java s2/C2485b.java s2/c.java u2/f.java u2/m.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	B/C0009d.java K7/f.java M7/o0.java e8/C1439b.java i0/W.java x6/b.java
6	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	Ad/f.java Bd/C0036f.java Kb/g.java Wb/b.java u5/AbstractC2702H.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	B/RunnableC0010e.java D5/C0099c.java D6/c.java E7/g.java H2/C0234q.java H2/h0.java J6/H1.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java ka/AbstractC1882a.java ka/C1883b.java ka/C1884c.java la/C1937a.java life/enerjoy/justfit/app/JustFitApplication.java t8/d.java u2/t.java x2/f.java x8/e.java x8/f.java y8/h.java y8/m.java z7/C2994a.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	K7/h.java o7/f.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	D5/A.java d0/C1303h.java f5/E.java f5/g.java m5/i.java s5/C2489b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Ca/l.java Ga/d.java Ha/c.java Rb/b.java Se/e.java Se/h.java Se/m.java Se/n.java Ua/c.java Ya/i.java fb/j.java ic/d.java ve/a.java
11	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	Ta/a.java
12	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	Z3/x.java xe/C2907d.java
13	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	Gb/m.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	Y8/b.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java
			Bd/g0.java C1/e.java C3/a.java C3/d.java C3/j.java E4/f.java G4/c.java G4/e.java H1/c.java J6/R0.java K7/h.java K7/n.java Ke/E.java L0/c.java L7/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
			L7/o.java O4/A.java P7/a.java Se/d.java
00013	Read file and put it into a stream	file	Y1/A.java Y1/F.java Ye/r.java a2/C0777e.java b2/i.java c/C1003d.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java ea/C1455j.java g/AbstractC1561a.java g5/g.java i0/W.java o4/CallableC2200j.java o5/k.java p5/C2267d.java s5/C2488a.java t2/C2562c.java t2/u.java wd/v.java xe/C2907d.java xe/e.java y4/C2949c.java
00012	Read data and put it into a buffer stream	file	E4/f.java g5/g.java o5/k.java
00004	Get filename and put it to JSON object	file collection	J6/R0.java K/g.java L0/c.java n2/C2102s.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java u5/AbstractC2719i.java u5/C2697C.java
00036	Get resource file from res/raw directory	reflection	B/RunnableC0014i.java Fb/b.java Md/d.java Ua/d.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java f4/C1492a.java g5/i.java life/enerjoy/justfit/module/ratealert/RateAlertFragment.java p5/g.java p6/f.java t2/u.java u3/C2678a.java u5/AbstractC2702H.java u5/AbstractC2719i.java u5/DialogC2710P.java
00014	Read file into a stream and put it into a JSON object	file	J6/R0.java L0/c.java L7/g.java com/appsflyer/internal/AFg1jSDK.java i0/W.java p5/C2267d.java s5/C2488a.java xe/C2907d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	i0/W.java kc/C1892g.java ze/C3010a.java ze/C3012c.java ze/C3013d.java ze/C3015f.java
00065	Get the country code of the SIM card provider	collection	c/C1003d.java w7/AbstractC2853b.java
00022	Open a file from given absolute path of the file	file	Ad/f.java Ae/a.java Kb/g.java L7/g.java Y1/F.java Y1/t.java Ya/b.java com/appsflyer/internal/AFg1jSDK.java g/AbstractC1561a.java o4/AbstractC2203m.java o4/CallableC2200j.java y4/C2949c.java
00189	Get the content of a SMS message	sms	Zc/d.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java
00188	Get the address of a SMS message	sms	Zc/d.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	Zc/d.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java
00201	Query data from the call log	collection calllog	Zc/d.java com/appsflyer/internal/AFi1bSDK.java u5/C2697C.java
00005	Get absolute path of file and put it to JSON object	file	L7/g.java com/appsflyer/internal/AFg1jSDK.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java u5/AbstractC2702H.java
00132	Query The ISO country code	telephony collection	J2/b.java c/C1003d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	B/RunnableC0014i.java D5/C0099c.java Fc/K.java J6/H1.java J6/U0.java Md/d.java Ua/d.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java life/enerjoy/justfit/module/ratealert/RateAlertFragment.java p6/f.java sb/g.java u3/B.java u3/C2678a.java u3/C2680c.java u5/AbstractC2702H.java u5/AbstractC2719i.java u5/C2697C.java u5/C2705K.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Fc/K.java Md/d.java life/enerjoy/justfit/module/ratealert/RateAlertFragment.java p6/f.java sb/g.java u3/C2678a.java u3/C2680c.java u5/AbstractC2702H.java u5/AbstractC2719i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	J6/RunnableC0312n0.java J6/U.java Ua/d.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bumptech/glide/load/data/k.java f6/h.java f8/c.java l6/C1916b.java o6/RunnableC2219c.java t2/o.java
00096	Connect to a URL and set request method	command network	Ua/d.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java f6/h.java q6/c.java t2/o.java
00089	Connect to a URL and receive input stream from the server	command network	Be/g.java Ua/d.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/k.java f6/h.java f8/c.java t2/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	D5/E.java E4/y.java J6/U0.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java u5/C2697C.java
00187	Query a URI and check the result	collection sms calllog calendar	u5/C2697C.java
00094	Connect to a URL and read data from it	command network	kc/C1893h.java t2/o.java
00114	Create a secure socket connection to the proxy address	network command	Oe/j.java
00024	Write file after Base64 decoding	reflection file	Bd/j0.java La/b.java o4/AbstractC2203m.java
00162	Create InetSocketAddress object and connecting to it	socket	Se/c.java Se/n.java
00163	Create new Socket and connecting to it	socket	Se/c.java Se/n.java
00112	Get the date of the calendar event	collection calendar	life/enerjoy/justfit/feature/workout/ui/WorkoutDoneClockInFragment.java wb/C2862a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	J6/U.java com/bumptech/glide/load/data/k.java q6/c.java t2/o.java
00028	Read file from assets directory	file	t2/C2560a.java
00108	Read the input stream from given URL	network command	J6/S.java J6/X0.java t2/o.java
00015	Put buffer stream (data) to JSON object	file	u5/AbstractC2702H.java
00171	Compare network operator with a string	network	u5/AbstractC2702H.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	life/enerjoy/justfit/feature/workout/ui/WorkoutDoneFragment.java
00121	Create a directory	file command	life/enerjoy/justfit/module/profile/photo/PhotoClipFragment.java
00147	Get the time of current location	collection location	q/v.java
00075	Get location of the device	collection location	q/v.java
00115	Get last known location of the device	collection location	q/v.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/21715440079/namespaces/firebase:fetch?key=AIzaSyCXP8nklCi6nPhbgDDS-0wMHPXQRoFT7k0. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, 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
www.googleadservices.com	ok	**IP:** 142.250.74.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
enerjoy.life	ok	**IP:** 18.238.96.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sars.s	ok	No Geolocation information available.
app-measurement.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
yaml.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 216.58.207.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
resource.justfit.app	ok	**IP:** 18.238.96.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
scdn-steststtings.s	ok	No Geolocation information available.
testsolution.enerjoy.life	ok	**IP:** 44.217.83.125 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
justfita.zendesk.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.62 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.143 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cdn.enerjoy.life	ok	**IP:** 18.155.173.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
google.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	p6/k.java
contact.justfit@enerjoy.life	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
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
"com.google.firebase.crashlytics.mapping_file_id" : "ab21a586c6f94b5f82cc2b273c34f9cd"
"facebook_client_token" : "7774a2d36180d5d1955957737a13076dab6c00b434fe87df8000e9256b6ed4f2"
"google_api_key" : "AIzaSyCXP8nklCi6nPhbgDDS-0wMHPXQRoFT7k0"
"google_crash_reporting_api_key" : "AIzaSyCXP8nklCi6nPhbgDDS-0wMHPXQRoFT7k0"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
470fa2b4ae81cd56ecbcda9735803434cec591fa
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cb69c804bce7e03e8b1ce4f297323f10

POSSIBLE SECRETS
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
b2627ee228643603bcb8c176dda3036f
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
d7b73ec8cf8f297218c1a65764f871a0
0f623429f3fefec1bdbb6deaaceb0262
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
f1968a47921a17415cd50e46b17da7db
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

POSSIBLE SECRETS
ffc830d0d484407eda20df0dd16bd820
b6f31aa9a9ce3138c365d8adabbd25c7
4ddb0db97bbacfacf40f6a891f31c189
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

PLAYSTORE INFORMATION

Title: JustFit - Lazy Workout

Score: 4.6933365 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** fitness.home.workout.weight.loss

Developer Details: ENERJOY PTE. LTD., 5785833978814606982, None, https://www.enerjoy.life/, service_android@support.justfit.app,

Release Date: Oct 25, 2022 **Privacy Policy:** Privacy link

Description:

Lose weight and gain muscle with no equipment. Follow the professional guide to enjoy health and fitness training. Embark on our new beginner wall pilates courses today. Let’s go with the JustFit App. JustFit is your science-backed virtual coach. It is time for you to start your training with a 28 day wall pilates challenge. JustFit has got everything ready. JustFit is leading the trend of wall pilates workouts, offering workouts like belly exercise for women that focus not just on losing fat but on overall well-being. For those new to this, our beginner wall pilates series offers easy-to-follow lessons and tips, making sure you get the hang of it with the best workout apps for beginners. The road to the top is here. Let’s go, let’s do it. JustFit will strictly track your daily progress. It is high time to get what you want. Transform your body with our professional workout plans and a huge library of exercises from beginner to advanced. Discover a wide range of exercises tailored to your needs. JustFit can give you personalized recommendations regarding your requirements and is here to assist you. Whether you want to target your training on focused areas, lose weight, gain muscle, or just seek easy health and fitness training. Change yourself by working out anytime and anywhere with the JustFit App. • Workouts at home at any time. We’ve got you covered with a variety of exercise sets for at-home sessions with zero equipment. • Tailor-made approach to weight loss and weight gain through targeted exercise. We analyze your profile preferences and lifestyle to help you achieve your goal faster. • Varied workouts adapted to your needs. We provide a wide range of workout exercises, you can find everything you like and start training anytime. Features: • Workout Coach: Personalized workout plan to help you get in shape faster • Wall Pilates Workouts: Try pilates with a new approach, using wall-based exercises for a better workout • Belly Exercise for Women: Focused belly fat workouts for women, designed for a strong and toned core • From Beginner to Advanced: Wide range of fitness and workout exercises to cover your personal needs • Target Training: Focus on problem areas adapted to your needs • Daily Progress Tracker: Track your everyday progress to meet your goal • Health & Fitness Tips: Explore our wide range

of health and fitness training resources, keeping you on the right track Join thousands of users who have transformed themselves with the JustFit App.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:17:31	Generating Hashes	OK
2025-09-01 13:17:32	Extracting APK	OK
2025-09-01 13:17:32	Unzipping	OK
2025-09-01 13:17:32	Parsing APK with androguard	OK
2025-09-01 13:17:33	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:17:33	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:17:35	Parsing AndroidManifest.xml	OK
2025-09-01 13:17:35	Extracting Manifest Data	OK

2025-09-01 13:17:35	Manifest Analysis Started	OK
2025-09-01 13:17:36	Performing Static Analysis on: JustFit (fitness.home.workout.weight.loss)	OK
2025-09-01 13:17:37	Fetching Details from Play Store: fitness.home.workout.weight.loss	OK
2025-09-01 13:17:39	Checking for Malware Permissions	OK
2025-09-01 13:17:39	Fetching icon path	OK
2025-09-01 13:17:39	Library Binary Analysis Started	OK
2025-09-01 13:17:39	Reading Code Signing Certificate	OK
2025-09-01 13:17:39	Running APKiD 2.1.5	OK
2025-09-01 13:17:42	Detecting Trackers	OK
2025-09-01 13:17:43	Decompiling APK to Java with JADX	OK
2025-09-01 13:17:56	Converting DEX to Smali	OK

2025-09-01 13:17:56	Code Analysis Started on - java_source	OK
2025-09-01 13:17:59	Android SBOM Analysis Completed	OK
2025-09-01 13:18:04	Android SAST Completed	OK
2025-09-01 13:18:04	Android API Analysis Started	OK
2025-09-01 13:18:12	Android API Analysis Completed	OK
2025-09-01 13:18:12	Android Permission Mapping Started	OK
2025-09-01 13:18:18	Android Permission Mapping Completed	OK
2025-09-01 13:18:18	Android Behaviour Analysis Started	OK
2025-09-01 13:18:28	Android Behaviour Analysis Completed	OK
2025-09-01 13:18:28	Extracting Emails and URLs from Source Code	OK

2025-09-01 13:18:32	Email and URL Extraction Completed	OK
2025-09-01 13:18:32	Extracting String data from APK	OK
2025-09-01 13:18:32	Extracting String data from Code	OK
2025-09-01 13:18:32	Extracting String values and entropies from Code	OK
2025-09-01 13:18:35	Performing Malware check on extracted domains	OK
2025-09-01 13:18:38	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.