MOBSF

ANDROID STATIC ANALYSIS REPORT

GENEFIT (3.4.401)

File Name: com.mightybell.threex4genetics.dtcmobile_401.apk

Package Name:	com.mightybell.threex4genetics.dtcmobile
Scan Date:	Aug. 31, 2025, 4:22 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	25	4	2	2

FILE INFORMATION

File Name: com.mightybell.threex4genetics.dtcmobile_401.apk
Size: 38.26MB
MD5: d306406b71036371af2c0e2e7b4c90c4
SHA1: 836923463a3e8da7b0e38ec76e9654ecc03114e5
SHA256: 8be645d68c34cff3bb99ffc14508c18b807a756e756fd40146c18c8eb481f87b

APP INFORMATION

App Name: GENEFIT
Package Name: com.mightybell.threex4genetics.dtcmobile
Main Activity: com.mightybell.threex4genetics.dtcmobile.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 3.4.401
Android Version Code: 401

APP COMPONENTS

Activities: 42
Services: 9

Receivers: 7
Providers: 7
Exported Activities: 8
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
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: 2023-09-13 09:48:07+00:00
Valid To: 2053-09-13 09:48:07+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x7c93817fb6c61381d1f7a248275a891696cf1578
Hash Algorithm: sha256
md5: 8e270bc5058571d75a6c91689a77c687
sha1: 3c69318f8090b7c7dee2699008a610e883243ca5
sha256: 20d7aa15231e94287eccfb9f932d79efe06e8171921179b5b2da2e8c525520fd
sha512: 8c7d734c3bd7202409b7ad2e2b8dcac1f235d292640ce7edf1499bfffac1757c38ac601ba62b2eb165f0dbe31a301e3cd7c9524f09d98e334156cbe7fed1c881
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 55796de7fe7d61712757750ae9238a2c997848c03653d1a58a1fb282462d7865
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.mightybell.threex4genetics.dtcmobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mightybell.threex4genetics.dtcmobile.MainActivity	Schemes: com.mightybell.threex4genetics.dtcmobile.garmin://, http://, https://, Hosts: 3x4genefit-dtc, 3x4genetics.io,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: com.mightybell.threex4genetics.dtcmobile://, Hosts: 3x4genefit-dtc,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.mightybell.threex4genetics.dtcmobile,

ACTIVITY	INTENT
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.mightybell.threex4genetics.dtcmobile,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.mightybell.threex4genetics.dtcmobile,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.mightybell.threex4genetics.dtcmobile/success, /com.mightybell.threex4genetics.dtcmobile/cancel, Path Prefixes: /com.mightybell.threex4genetics.dtcmobile/authentication_return, /com.mightybell.threex4genetics.dtcmobile,

NETWORK SECURITY

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: 13 | 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	Activity (net.openid.appauth.RedirectUriReceiverActivity) 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 (id.flutter.flutter_background_service.BackgroundService) is not Protected. [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.
5	Broadcast Receiver (id.flutter.flutter_background_service.WatchdogReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (id.flutter.flutter_background_service.BootReceiver) 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	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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.
8	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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.
9	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.
10	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
11	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
12	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
14	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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b2/i.java b2/v0.java be/e.java bh/u.java com/appsflyer/appsflyersdk/AppsFlyerConstants.java com/stripe/android/financialconnections/a.java com/stripe/android/financialconnections/model/FinancialConnectionsSession.java com/stripe/android/model/Source.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/b.java com/stripe/android/model/c.java com/stripe/android/model/f.java com/stripe/android/model/l.java com/stripe/android/model/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/stripe/android/model/r.java com/stripe/android/model/v.java com/stripe/android/model/y.java com/stripe/android/payments/bankaccount/ui/a.java com/stripe/android/payments/core/authentication/threeds2/c.java com/stripe/android/payments/paymentlauncher/c.java com/stripe/android/paymentsheet/addresselement/a.java com/stripe/android/paymentsheet/m.java com/stripe/android/paymentsheet/paymentdatacollection/polling/b.java com/stripe/android/paymentsheet/paymentdatacollection/polling/c.java dh/a.java e0/w0.java fj/a.java hm/a.java hm/c.java hm/c0.java kk/e0.java kk/m.java kk/u.java kk/w.java l0/o1.java l0/p2.java m4/g.java o4/d.java o4/p.java o4/x.java ok/c.java ok/d.java qh/k.java rl/c.java sk/a.java sl/a.java sn/p7.java ti/b.java xl/c.java xm/i.java yi/c.java zi/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a6/e0.java a6/i.java a6/m0.java ac/d.java af/h.java af/o.java ao/f.java aq/f0.java aq/h.java as/a.java b4/a.java b5/e.java b5/f.java b5/p.java b5/r.java b7/a.java bc/b.java bf/a.java bg/a.java bg/e.java c2/f0.java c3/c.java c4/e0.java c5/d.java cg/h.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1hSDK.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/stripe/hcaptcha/webview/HCaptchaWebView.java cq/q.java dc/g.java dd/f.java dg/a.java dn/b.java dp/b.java dq/g0.java ds/d.java eq/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	f/e.java f5/d.java f5/j.java fb/e.java fq/l.java ga/g.java gq/j.java gu/j.java hm/e0.java i2/c.java id/flutter/flutter_background_service/BackgroundService.java io/sentry/android/core/u.java io/sentry/android/replay/s.java io/sentry/android/replay/v.java io/sentry/flutter/SentryFlutter$updateOptions$24.java io/sentry/r6.java j4/a.java j4/n.java j4/o.java j4/p.java j5/a.java j6/c.java jh/d.java k4/a.java k5/g.java k5/i0.java k5/n0.java k5/s0.java kb/h.java kd/e.java kn/c0.java kn/e0.java kn/i.java l4/d.java l4/e.java l5/c.java l5/f.java la/a.java ld/b.java m7/k.java md/b.java ms/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n2/d.java n3/d.java n4/c.java n4/e.java na/a.java o3/c.java o3/d.java o3/e.java o4/i.java o4/q.java o4/z.java oa/g.java oa/q.java om/r1.java p4/i.java p4/j.java p5/e.java p5/f.java p7/a.java q2/f.java q3/a.java q4/e.java q4/i.java r4/a.java r5/a.java ra/j.java s2/a.java s4/c.java s4/d.java s4/f.java s4/s.java s4/t.java sa/b.java sd/c1.java sd/d0.java sd/f0.java sd/f1.java sd/m0.java sd/s0.java sd/t1.java sd/z.java sn/z7.java t5/i.java t5/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				td/g.java td/j.java te/b.java th/h.java u3/c.java u4/a.java u9/r.java uc/a.java uc/b.java uc/c.java ue/c.java v3/a.java v4/b0.java v4/c.java v4/d.java v4/k.java v4/m.java v4/n.java v4/r.java v4/z.java v6/b.java w3/a.java w3/m.java w6/a.java wd/f.java wg/j0.java x0/c.java x0/g.java x1/s.java xa/f.java y2/c.java y9/a.java y9/d.java ya/f0.java z4/a.java z4/d.java z4/j.java z9/o.java za/e.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	zd/r.java zg/j.java l5/d.java sn/s1.java t5/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/d.java
5	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	cg/h.java e9/a.java sn/k7.java
6	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	a6/l0.java c9/b.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1fSDK.java k5/r.java y7/q1.java z8/p0.java zq/a.java
7	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	a6/l0.java ao/c.java eq/i.java eq/j.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	k5/b.java k5/j.java k5/p0.java k5/t0.java r5/j.java x5/b.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ls/c.java ls/d.java ls/g.java ls/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	lg/a.java mt/e.java vs/a.java ws/a.java xs/a.java ys/a.java
11	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	cb/b.java te/c.java
12	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	kn/i.java t7/m0.java t7/t0.java
13	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	io/sentry/util/u.java j6/a.java te/b.java
14	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java zd/i.java
15	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	ae/d.java c6/k.java ge/a.java sn/h9.java sn/s1.java te/c.java u5/j.java x5/a.java
00022	Open a file from given absolute path of the file	file	a7/a.java ae/d.java ao/c.java ao/f.java eq/j.java io/sentry/android/replay/g.java io/sentry/cache/c.java io/sentry/p.java io/sentry/p5.java io/sentry/w.java sn/f9.java sn/s1.java v6/a.java v6/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ae/d.java c6/k.java com/appsflyer/internal/AFb1iSDK.java com/bumptech/glide/load/a.java dg/a.java ee/e.java ge/a.java io/sentry/android/replay/g.java io/sentry/cache/c.java io/sentry/config/e.java io/sentry/util/e.java io/sentry/w.java k4/a.java l5/f.java ps/m.java s4/f.java sn/a6.java sn/b6.java sn/h9.java sn/s1.java t5/l.java t9/h.java t9/k0.java te/c.java tq/j.java ts/d2.java u5/j.java v6/b.java x5/a.java zd/a0.java
00005	Get absolute path of file and put it to JSON object	file	ae/d.java ao/f.java sn/s1.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00012	Read data and put it into a buffer stream	file	io/sentry/config/e.java io/sentry/util/e.java io/sentry/w.java l5/f.java sn/a6.java t5/l.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/j.java hm/j0.java j6/c.java t9/u.java ue/c.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a6/a.java a6/e0.java a6/l0.java a6/m0.java a6/q0.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/view/v1.java cq/l.java di/a.java g4/a.java gq/i.java j4/a.java j4/n.java j4/p.java net/openid/appauth/c.java w3/a.java w3/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a6/l0.java a6/m0.java com/stripe/android/link/LinkForegroundActivity.java di/a.java g4/a.java gq/i.java j4/a.java j4/n.java j4/p.java w3/a.java
00078	Get the network operator name	collection telephony	a6/l0.java ao/f.java com/appsflyer/internal/AFi1xSDK.java
00004	Get filename and put it to JSON object	file collection	ao/f.java c6/c.java g6/a.java sn/a9.java sn/s1.java u5/f.java
00003	Put the compressed bitmap data into JSON object	camera	k5/i0.java sn/f6.java
00036	Get resource file from res/raw directory	reflection	a6/a.java a6/l0.java a6/m0.java a6/q0.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java j4/a.java j4/n.java t9/k0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java hm/j0.java k5/i0.java qh/m.java t9/u.java ue/c.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/j.java ga/f.java hm/j0.java t9/u.java ue/c.java vk/i.java y9/d.java
00091	Retrieve data from broadcast	collection	a6/e0.java com/appsflyer/internal/AFc1vSDK.java com/stripe/android/link/LinkForegroundActivity.java net/openid/appauth/AuthorizationManagementActivity.java
00015	Put buffer stream (data) to JSON object	file	a6/l0.java
00009	Put data in cursor to JSON object	file	a6/l0.java
00191	Get messages in the SMS inbox	sms	a6/a.java a6/e0.java a6/l0.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	a6/e0.java com/appsflyer/internal/AFb1jSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	a6/e0.java com/appsflyer/internal/AFb1jSDK.java n4/c.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java hm/j0.java t9/u.java
00094	Connect to a URL and read data from it	command network	de/a.java t9/u.java
00108	Read the input stream from given URL	network command	t9/u.java
00162	Create InetSocketAddress object and connecting to it	socket	ls/b.java ls/h.java
00163	Create new Socket and connecting to it	socket	ls/b.java ls/h.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/i.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/i.java
00189	Get the content of a SMS message	sms	a6/e0.java
00188	Get the address of a SMS message	sms	a6/e0.java
00200	Query data from the contact list	collection contact	a6/e0.java
00187	Query a URI and check the result	collection sms calllog calendar	a6/e0.java
00201	Query data from the call log	collection calllog	a6/e0.java
00202	Make a phone call	control	j4/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	j4/p.java
00125	Check if the given file path exist	file	u5/f.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	z6/a.java
00132	Query The ISO country code	telephony collection	u9/n0.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/h.java
00028	Read file from assets directory	file	t9/c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://x4-genetics---dtc-mobile-app-default-rtdb.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1065612840643/namespaces/firebase:fetch?key=AIzaSyA9pABkq17J9fC8a42c_2u7qicZxmDs4Es is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'action_workouts_delete': 'true', 'available_link_devices': 'garmin,apple,polar', 'available_social_logins': 'facebook,apple,google', 'env_application_tag': 'dtc', 'env_appsflyer_app_id_android': 'com.mightybell.threex4genetics.dtcmobile', 'env_appsflyer_app_id_ios': '6466628036', 'env_appsflyer_dev_key_android': 'k57vDW3m9jc6jBjVUuattN', 'env_appsflyer_dev_key_ios': 'k57vDW3m9jc6jBjVUuattN', 'env_base_auth_url': 'https://auth.3x4genetics.com/', 'env_base_graph_url': 'https://xwpctr6iqrfohj6f7t5jud2wge.appsync-api.us-east-2.amazonaws.com/graphql', 'env_base_graph_url_genefit': 'https://api.genefit.ai/graphql', 'env_base_graph_url_genefit_af_south_1': 'https://af-south-1.api.genefit.ai/graphql', 'env_base_graph_url_genefit_eu_west_1': 'https://eu-west-1.api.genefit.ai/graphql', 'env_base_graph_url_genefit_us_east_2': 'https://api.genefit.ai/graphql', 'env_base_reset_password_url': 'https://auth.3x4genetics.com/reset-password/genefit', 'env_client_id': 'fitness:dtc', 'env_client_secret': 'Fc2PBX33rKuG6JAW', 'env_debug_login_users': '', 'env_privacy_url': 'https://genefit.pro/privacy-policy', 'env_release_type': 'PROD', 'env_stripe_merchant_id': 'com.mightybell.threex4genetics.dtcmobile.stripe', 'env_stripe_publish_key': 'pk_live_20Rj8GsFpiyMyCK2mRONVG5w00L3lvWAtg', 'env_stripe_url_scheme': '3x4genefit-dtc', 'env_team': '3x4_Test', 'env_terms_conditions_url': 'https://genefit.pro/terms-of-service', 'env_translations_api_key': 'f25rtAwTfPw4CJehBaXgSB4oW3uqdsfE', 'env_translations_url': 'https://translations.genefit.ai/{LOCALE}.json', 'env_uxcam_tracking_id': 'u3g9uo4nsfyhgni', 'fe_navigation_map': '[{ "tab": "dashboard", "id": "000", "label": "menu_dashboard", "route": "dashboard" }, { "tab": "performance", "id": "100", "label": "menu_performance", "route": "performance" }, { "tab": "genetics", "id": "200", "label": "menu_genetics", "route": "genetics" }, { "tab": "training", "id": "300", "label": "menu_training", "route": "training" }, { "tab": "profile", "id": "400", "label": "menu_profile", "route": "profile" }]', 'fe_performance_graph_granularity': 'threeMonths', 'genetics_kit_price': '199.00', 'genetics_no_kit_learn_more': 'https://genefit.pro/pages/the-power-of-your-genetics', 'health_sync_days_batch': '10', 'health_sync_days_history': '50', 'key_workouts_cloud_map_id': 'cc58744e3b895651', 'key_workouts_cloud_map_id_android': 'cc58744e3b895651', 'key_workouts_cloud_map_id_ios': '950ba2fc9279583c', 'kit_order_allowed_regions': 'us-east-2,af-south-1,eu-west-1', 'new_user_register_enabled': 'true', 'subscription_allowed_regions': 'us-east-2'}, 'state': 'UPDATE', 'templateVersion': '37'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
link.com	ok	**IP:** 52.89.224.113 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **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.

DOMAIN	STATUS	GEOLOCATION
api.stripe.com	ok	**IP:** 54.149.153.72 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
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
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
errors.stripe.com	ok	**IP:** 198.137.150.161 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
verify-region.uxcam.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
x4-genetics---dtc-mobile-app-default-rtdb.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.250.72.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.stripe.com	ok	**IP:** 34.215.30.129 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.101.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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:** 184.50.27.48 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
slaunches.s	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
hooks.stripe.com	ok	**IP:** 54.187.175.68 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
stripe.com	ok	**IP:** 35.167.54.49 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
q.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sapp.s	ok	No Geolocation information available.
verify-stg.uxcam.com	ok	**IP:** 35.82.4.56 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **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:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
r.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	lh/a.java
support@stripe.com	qh/k.java
support@stripe.com	nk/f.java
support@stripe.com	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
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447
UXCam	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/253

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "7d78d5c8d5f7bbc016c184d6c0fb13d9"
"firebase_database_url" : "https://x4-genetics---dtc-mobile-app-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyA9pABkq17J9fC8a42c_2u7qicZxmDs4Es"
"google_crash_reporting_api_key" : "AIzaSyA9pABkq17J9fC8a42c_2u7qicZxmDs4Es"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
115792089237316195423570985008687907853269984665640564039457584007908834671663
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

POSSIBLE SECRETS
41058363725152142129326129780047268409114441015993725554835256314039467401291
nhJzkFTHpvSqjxfqTbLepDkhInppZDMvpX6INOBGZQwEdaV37QgLp6cgfsK2oRhur
470fa2b4ae81cd56ecbcda9735803434cec591fa
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDNUf8CVU/4PRJebkLWYKQIMAiN
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
dcb428fea25c40e7b99f81ae5981ee6a
3267051002075881697808308513050704318447127338065924327593890433575733748242 4
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c56fb7d591ba6704df047fd98f535372fea00211
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291 115057148
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748 8478985984
deca87e736574c5c83c07314051fd93a

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
55066263022277343669578718895168534326250603453777594175500187360389116729240
484395612939064517590525852527979142027629495260417479958440807171082404635286
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
1157920892373161954235709850086879078528375642790749043826051631415181614943 37
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599846
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
115792089210356248762697446949407573530086143415290314195533631308867097853948
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: GENEFIT

Score: 3.99 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.mightybell.threex4genetics.dtcmobile

Developer Details: 3X4 Genetics, 3X4+Genetics, None, https://www.genefit.pro, support@genefit.ai,

Release Date: Nov 1, 2023 **Privacy Policy:** Privacy link

Description:

GENEFIT leverages your unique genetic blueprint to revolutionize your workout experience. Our app doesn't just track your fitness; it transforms it by intertwining your DNA with every aspect of your training. We help you... Optimize Workouts: Receive tailored training plans, ensuring every session is as effective as possible. Avoid Injuries: With real-time tissue health monitoring and injury risk alerts, stay safe and sustain your fitness journey. Maximize Performance: Uncover your innate genetic strengths and weaknesses to excel in six key athletic categories. With... Daily Health Monitoring: Keep a close watch on your tissue health, getting alerted at the first sign of potential overuse. Genetic Insight Discovery: Dive deep into your genetic makeup to understand and exploit your natural athletic inclinations. Personalized Training Adaptation: Adapt your training to your genetic profile, constantly evolving as you do. Progress Tracking: Monitor your advancements with sophisticated, genetics-informed metrics. Nutritional and Lifestyle Guidance: Receive customized recommendations to support your training and recovery, based on your genetics and current fitness level.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 04:22:37	Generating Hashes	OK
2025-08-31 04:22:37	Extracting APK	OK
2025-08-31 04:22:37	Unzipping	OK
2025-08-31 04:22:38	Parsing APK with androguard	OK
2025-08-31 04:22:38	Extracting APK features using aapt/aapt2	OK

2025-08-31 04:22:42	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 04:22:45	Parsing AndroidManifest.xml	OK
2025-08-31 04:22:45	Extracting Manifest Data	OK
2025-08-31 04:22:45	Manifest Analysis Started	OK
2025-08-31 04:22:45	Performing Static Analysis on: GENEFIT (com.mightybell.threex4genetics.dtcmobile)	OK
2025-08-31 04:22:46	Fetching Details from Play Store: com.mightybell.threex4genetics.dtcmobile	OK
2025-08-31 04:22:46	Checking for Malware Permissions	OK
2025-08-31 04:22:46	Fetching icon path	OK
2025-08-31 04:22:46	Library Binary Analysis Started	OK
2025-08-31 04:22:46	Reading Code Signing Certificate	OK
2025-08-31 04:22:47	Running APKiD 2.1.5	OK
2025-08-31 04:22:55	Detecting Trackers	OK

2025-08-31 04:22:58	Decompiling APK to Java with JADX	OK
2025-08-31 04:48:19	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/d306406b71036371af2c0e2e7b4c90c4/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/d306406b71036371af2c0e2e7b4c90c4/d306406b71036371af2c0e2e7b4c90c4.apk'], 999.9999834150076)
2025-08-31 04:48:19	Converting DEX to Smali	OK
2025-08-31 04:48:19	Code Analysis Started on - java_source	OK
2025-08-31 04:48:24	Android SBOM Analysis Completed	OK
2025-08-31 04:48:36	Android SAST Completed	OK
2025-08-31 04:48:36	Android API Analysis Started	OK
2025-08-31 04:48:47	Android API Analysis Completed	OK
2025-08-31 04:48:48	Android Permission Mapping Started	OK
2025-08-31 04:48:52	Android Permission Mapping Completed	OK
2025-08-31 04:48:52	Android Behaviour Analysis Started	OK

2025-08-31 04:49:05	Android Behaviour Analysis Completed	OK
2025-08-31 04:49:05	Extracting Emails and URLs from Source Code	OK
2025-08-31 04:49:08	Email and URL Extraction Completed	OK
2025-08-31 04:49:08	Extracting String data from APK	OK
2025-08-31 04:49:08	Extracting String data from Code	OK
2025-08-31 04:49:08	Extracting String values and entropies from Code	OK
2025-08-31 04:49:12	Performing Malware check on extracted domains	OK
2025-08-31 04:49:14	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.