ANDROID STATIC ANALYSIS REPORT

No icon

Benefits (18.0.0)

File Name:	com.lighthouse1.mobilebenefits.dbi_181.apk
Package Name:	com.lighthouse1.mobilebenefits.dbi
Scan Date:	Aug. 31, 2025, 1 a.m.
App Security Score:	62/100 (LOW RISK)
Grade:	A
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	17	1	6	1

FILE INFORMATION

File Name: com.lighthouse1.mobilebenefits.dbi_181.apk
Size: 10.27MB
MD5: b3250d542a1a0a894426e52d7d841698
SHA1: 6e284d06415bb9c45cfa6dc97c004bdf826bd72b
SHA256: 888d4f400f3f3dee64e1ba2eb56227c79b6baa969c57ec64f98a8e5cb047c85c

APP INFORMATION

App Name: Benefits
Package Name: com.lighthouse1.mobilebenefits.dbi
Main Activity: com.lighthouse1.mobilebenefits.activity.LoginActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 18.0.0

Android Version Code: 181

APP COMPONENTS

Activities: 80
Services: 7
Receivers: 5
Providers: 4
Exported Activities: 2
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=Minnesota, L=Minneapolis, O=Lighthouse1, OU=Lighthouse1, CN=Lighthouse1
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-11-11 15:06:16+00:00
Valid To: 2038-03-29 15:06:16+00:00
Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Lighthouse1, OU=Lighthouse1, CN=Lighthouse1
Serial Number: 0x4cdc0668
Hash Algorithm: sha1
md5: 68a51bd43442347a1f3d1f8bd9d8ea76
sha1: 6d6f473d786903ef4f3436c4891f19856d675e1b
sha256: 26fd8fa91df95d791dd247eb778e9a9f475ed74036f5c8b17f5524c2215bb792
sha512: d4ddc312155741826f2e3acc4be041cd1917a5f2f14465f7111d65c01dbb9d0fdabc7e798ffcf502ba3344487c529c47686e18de431ef66ebf977074e7e7f60b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7c132cd16034847a4a762e91c99d164eeac7805be668f54eb69cd27b3abce3d0
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.lighthouse1.mobilebenefits.dbi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

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>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.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<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.BOARD check
SIM operator check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.lighthouse1.mobilebenefits.activity.LoginActivity	Schemes: evolution1.1mobile.dbi://,
sdk.pendo.io.activities.PendoGateActivity	Schemes: @string/PendoSchemeId://,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: com.lighthouse1.mobilebenefits.dbi.appauth://,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **3**

NO	SCOPE	SEVERITY	DESCRIPTION
1	evolution1.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: zy2aAVLUjYuPNpGj40vHiHjlWzaJvfcu+40NqwNeH3w= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: jyuGlAWoUrnZeQTtLngupkmucYkYjiJKm5q4wGo1w+o= Digest: SHA-256,Pin: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U= Digest: SHA-256]
2	navigatorsuite.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: jvYnGmScj1qAwz1odQPbLQJLUv+OtfUSGhIognqT4+E= Digest: SHA-256,Pin: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: EQOp9SQjE5F2HbMTYycxQMDmsNYTaNAl9MfqNbEtqf0= Digest: SHA-256]
3	lh1ondemand.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: pmzBene/Qc/GqiEaezhAZpeZo954t+OMW/swW5F5s6w= Digest: SHA-256,Pin: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: yE0wyyMmZu5v+C8jx+sXfVNK3tDhDTZjzaPDm5tSsIw= Digest: SHA-256]

CERTIFICATE ANALYSIS

HIGH: **1** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **5** | 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (sdk.pendo.io.activities.PendoGateActivity) 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	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.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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: **10** | INFO: **1** | SECURE: **3** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/e.java a2/i.java a4/b.java ab/n.java ab/s.java ab/t.java android/view/result/ActivityResultRegistry.java b2/a.java b5/h.java b6/a.java b6/b.java b6/c.java c2/c.java c2/d.java c2/g.java c2/t.java c2/u.java c2/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c4/b.java c4/d.java c4/f.java c4/h.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvvccvv.java com/lexisnexisrisk/threatmetrix/rl/tmxprofilingconnections/ujjuuuu.java com/samsung/android/sdk/samsungpay/enrollment/EnrollmentManager.java com/samsung/android/sdk/samsungpay/payment/PaymentManager.java com/samsung/android/sdk/samsungpay/v2/ApiLevelTable.java com/samsung/android/sdk/samsungpay/v2/BindRetry.java com/samsung/android/sdk/samsungpay/v2/PartnerRequest.java com/samsung/android/sdk/samsungpay/v2/RequestTracker.java com/samsung/android/sdk/samsungpay/v2/SamsungPay.java com/samsung/android/sdk/samsungpay/v2/SamsungPayBase.java com/samsung/android/sdk/samsungpay/v2/ServiceHelper.java com/samsung/android/sdk/samsungpay/v2/SpaySdk.java com/samsung/android/sdk/samsungpay/v2/SpayValidity.java com/samsung/android/sdk/samsungpay/v2/StubBase.java com/samsung/android/sdk/samsungpay/v2/VersionChecker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/samsung/android/sdk/samsungpay/v2/WatchManager.java com/samsung/android/sdk/samsungpay/v2/card/CardManager.java com/samsung/android/sdk/samsungpay/v2/payment/MstManager.java com/samsung/android/sdk/samsungpay/v2/payment/PaymentManager.java com/samsung/android/sdk/samsungpay/v2/service/ServiceManager.java com/samsung/android/sdk/samsungpay/v2/service/UserInfoCollection.java com/visa/mobileEnablement/pushProvisioning/l/d.java com/visa/mobileEnablement/pushProvisioning/p/b.java d1/b.java d1/v.java e0/d.java e2/a.java external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log$$serializer.java external/sdk/pendo/io/glide/a.java external/sdk/pendo/io/glide/gifdecoder/StandardGifDecoder.java external/sdk/pendo/io/glide/gifdecoder/d.java external/sdk/pendo/io/glide/load/data/AssetPathFetcher.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/glide/load/data/LocalUriFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/c.java external/sdk/pendo/io/glide/load/engine/Engine.java external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruArrayPool.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	external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruBitmapPool.java external/sdk/pendo/io/glide/load/engine/cache/DiskLruCacheWrapper.java external/sdk/pendo/io/glide/load/engine/g.java external/sdk/pendo/io/glide/load/engine/h.java external/sdk/pendo/io/glide/load/engine/n.java external/sdk/pendo/io/glide/load/engine/u.java external/sdk/pendo/io/glide/load/model/ByteBufferEncoder.java external/sdk/pendo/io/glide/load/model/ByteBufferFileLoader.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/glide/load/model/ResourceLoader.java external/sdk/pendo/io/glide/load/model/StreamEncoder.java external/sdk/pendo/io/glide/load/resource/ImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapEncoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/DefaultImageHeaderParser.java external/sdk/pendo/io/glide/load/resource/bitmap/VideoDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/b.java external/sdk/pendo/io/glide/load/resource/bitmap/c.java external/sdk/pendo/io/glide/load/resource/bitmap/d.java external/sdk/pendo/io/glide/load/resource/gif/ByteBufferGifDecoder.java external/sdk/pendo/io/glide/load/resource/gif/GifDrawableEncoder.java external/sdk/pendo/io/glide/load/resource/gif/StreamGifDecoder.java external/sdk/pendo/io/glide/manager/DefaultCo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				external/sdk/pendo/io/glide/manager/DefaultConnectivityMonitorFactory.java external/sdk/pendo/io/glide/manager/b.java external/sdk/pendo/io/glide/request/SingleRequest.java external/sdk/pendo/io/glide/request/target/CustomViewTarget.java external/sdk/pendo/io/glide/request/target/ViewTarget.java external/sdk/pendo/io/mozilla/javascript/Interpreter.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java f0/c.java f0/l.java f0/o.java f2/c.java f2/c0.java f2/d.java f2/k.java f2/m.java f2/n.java f2/r.java f2/z.java g1/a.java g6/c.java h0/f.java i4/z.java i6/g.java i6/n.java j1/j.java j2/a.java j2/d.java j2/j.java k0/b.java k0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k0/c.java k0/e.java k1/d.java l1/a.java l2/d.java l3/a.java l3/d.java l3/e.java l3/n.java l3/p.java l3/q.java n2/i.java n5/d.java nf/a.java o1/b.java o2/d.java o2/j.java o3/a0.java p4/f.java pf/d.java q0/d.java q3/b.java q3/b0.java q3/d.java q3/g0.java q3/u.java q3/x.java q5/h.java s0/c.java s2/a.java sdk/pendo/io/PendoInternal.java sdk/pendo/io/activities/PendoGateActivity.java sdk/pendo/io/c0/j.java sdk/pendo/io/c0/k.java sdk/pendo/io/c0/m.java sdk/pendo/io/c0/n.java sdk/pendo/io/g3/c.java sdk/pendo/io/h0/a.java sdk/pendo/io/j0/a.java sdk/pendo/io/logging/PendoLogger.java sdk/pendo/io/logging/c.java sdk/pendo/io/p/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sdk/pendo/io/p/a.java sdk/pendo/io/q8/a.java sdk/pendo/io/s7/e.java sdk/pendo/io/u6/g.java sdk/pendo/io/v/a.java sdk/pendo/io/w/a.java sdk/pendo/io/w/b.java sdk/pendo/io/x2/b.java sdk/pendo/io/y/b.java sdk/pendo/io/z7/a.java t1/a.java t5/i.java u1/a.java u4/a.java u6/b.java v1/d.java v1/e.java v3/b.java v6/c.java w/u0.java w2/k.java w3/e.java w3/o.java x1/c.java x1/e.java y0/c.java y1/h.java y1/i.java y1/k.java y1/q.java y1/z.java y2/a.java y4/a.java z1/i.java z1/j.java zf/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java sdk/pendo/io/a4/b.java sdk/pendo/io/b4/b.java sdk/pendo/io/d4/b.java sdk/pendo/io/e4/d.java sdk/pendo/io/e4/f.java sdk/pendo/io/e4/k.java sdk/pendo/io/f4/h.java sdk/pendo/io/j/b.java sdk/pendo/io/j/j.java sdk/pendo/io/k/i.java sdk/pendo/io/n3/b.java sdk/pendo/io/o3/a.java sdk/pendo/io/r3/a.java sdk/pendo/io/s3/a.java sdk/pendo/io/v3/b.java sdk/pendo/io/x3/a.java sdk/pendo/io/y3/a.java sdk/pendo/io/z3/a.java ya/a.java
				ab/c.java com/lighthouse1/mobilebenefits/fragment/AcceptDocumentFragment.java com/lighthouse1/mobilebenefits/fragment/HsaTransactionAccountsFragment.java com/lighthouse1/mobilebenefits/fragment/agreements/ViewAgreementDtoFragment.java com/lighthouse1/mobilebenefits/webservice/datacontract/consumer/ConsumerLoginStatus.java com/lighthouse1/mobilebenefits/webservice/datacontract/consumer/ListContent.java com/lighthouse1/mobilebenefits/webservice/datacontract/consumer/ListItemContent.java com/lighthouse1/mobilebenefits/webservice/datacontract/consumer/RsaActivityType.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log.java external/sdk/pendo/io/glide/load/engine/c.java external/sdk/pendo/io/glide/load/engine/m.java external/sdk/pendo/io/glide/load/engine/s.java external/sdk/pendo/io/mozilla/javascript/ClassCache.java external/sdk/pendo/io/mozilla/javascript/NativeError.java external/sdk/pendo/io/mozilla/javascript/NativeJavaObject.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/xmlimpl/XmlNode.java sdk/pendo/io/actions/ActivationManager.java sdk/pendo/io/actions/FloatingVisualGuide.java sdk/pendo/io/actions/ToolTipVisualGuide.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java sdk/pendo/io/d1/e.java sdk/pendo/io/m/LogServer.java sdk/pendo/io/models/GlobalEventPropertiesKt.java sdk/pendo/io/models/StepModel.java sdk/pendo/io/n/b.java sdk/pendo/io/q/g.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java w1/g.java y1/d.java y1/p.java y1/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	sdk/pendo/io/f3/c.java sdk/pendo/io/f3/d.java sdk/pendo/io/f3/g.java sdk/pendo/io/f3/h.java sdk/pendo/io/k/d.java sdk/pendo/io/t4/c.java sdk/pendo/io/t4/p0.java yf/c.java yf/d.java yf/i.java yf/j.java
5	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	android/view/result/ActivityResultRegistry.java com/distil/protection/android/Protection.java com/distil/protection/android/setAccessibilityPaneTitle.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/oddodod.java com/lexisnexisrisk/threatmetrix/rl/tmxprofilingconnections/ujuuuju.java com/visa/mobileEnablement/displayCard/b/a.java com/visa/mobileEnablement/pushProvisioning/b.java lc/a.java sdk/pendo/io/j3/d.java sdk/pendo/io/j3/h.java sdk/pendo/io/j4/f.java sdk/pendo/io/v4/c.java sdk/pendo/io/v4/d.java sdk/pendo/io/w2/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	external/sdk/pendo/io/daimajia/BuildConfig.java
7	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	ab/q.java ab/r.java w9/e0.java w9/f0.java
8	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	ab/u.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/odddodo.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvvvvcc.java sdk/pendo/io/q8/m.java u6/b.java
9	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	c3/b0.java c3/h0.java k1/c.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ab/r.java t5/w.java w9/e0.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	u6/c.java y8/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/lighthouse1/mobilebenefits/fragment/NewUserFragment.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java
13	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	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvvvcc.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Main.java
14	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	sdk/pendo/io/PendoInternal.java sdk/pendo/io/b8/a.java
15	This App uses SafetyNet API.	secure	OWASP MASVS: MSTG-RESILIENCE-7	gb/h.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java k1/d.java sdk/pendo/io/q8/h.java
00013	Read file and put it into a stream	file	app/tango/o/setOnApplyWindowInsetsListener.java c2/g.java com/bumptech/glide/load/a.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/uurruuu.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvvvcvc.java com/lighthouse1/mobilebenefits/webservice/i.java com/visa/mobileEnablement/displayCard/ah/b.java dg/n.java external/sdk/pendo/io/glide/load/a.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/mozilla/javascript/tools/SourceReader.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java fc/l.java g1/b.java sdk/pendo/io/p/a.java sdk/pendo/io/q8/h.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java u1/a.java u6/c.java w9/q.java
00131	Get location of the current GSM and put it into JSON	collection location	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java
00078	Get the network operator name	collection telephony	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java sdk/pendo/io/v7/e.java
00004	Get filename and put it to JSON object	file collection	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java sdk/pendo/io/q8/g.java
00085	Get the ISO country code and put it into JSON	collection telephony	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java
00099	Get location of the current GSM and put it into JSON	collection location	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java
00016	Get location info of the device and put it to JSON object	location collection	ab/d.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java
00132	Query The ISO country code	telephony collection	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vcvvvvv.java
00162	Create InetSocketAddress object and connecting to it	socket	com/lexisnexisrisk/threatmetrix/rl/tmxprofilingconnections/ujujuuu.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java yf/b.java yf/j.java
00163	Create new Socket and connecting to it	socket	com/lexisnexisrisk/threatmetrix/rl/tmxprofilingconnections/ujjjuuu.java com/lexisnexisrisk/threatmetrix/rl/tmxprofilingconnections/ujujuuu.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java yf/b.java yf/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/lighthouse1/mobilebenefits/activity/BaseActivity.java com/lighthouse1/mobilebenefits/activity/LoginActivity.java com/lighthouse1/mobilebenefits/activity/ScreenActivity.java com/lighthouse1/mobilebenefits/activity/SmartScanEobScanFormActivity.java com/lighthouse1/mobilebenefits/fragment/AcceptDocumentFragment.java com/lighthouse1/mobilebenefits/fragment/ScreenBaseFragment.java com/lighthouse1/mobilebenefits/view/BottomNavigation.java com/samsung/android/sdk/samsungpay/v2/SamsungPay.java com/samsung/android/sdk/samsungpay/v2/WatchManager.java com/visa/mobileEnablement/pushProvisioning/p/b.java net/openid/appauth/d.java q3/k0.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java w9/v.java y8/i.java
00023	Start another application from current application	reflection control	com/samsung/android/sdk/samsungpay/payment/PaymentManager.java com/samsung/android/sdk/samsungpay/v2/SpayValidity.java
00091	Retrieve data from broadcast	collection	com/lighthouse1/mobilebenefits/presentation/screen/rsachallenge/RsaOtpChallengeActivity.java com/visa/mobileEnablement/featureModuleCore/pushProvisioning/ui/headless/SpinnerActivity.java net/openid/appauth/AuthorizationManagementActivity.java w9/v.java
00130	Get the current WIFI information	wifi collection	ab/b.java com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvcvccv.java sdk/pendo/io/v7/d.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/lighthouse1/mobilebenefits/fragment/AcceptDocumentFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/lighthouse1/mobilebenefits/fragment/AcceptDocumentFragment.java
00147	Get the time of current location	collection location	ab/k.java
00075	Get location of the device	collection location	ab/k.java
00047	Query the local IP address	network collection	sdk/pendo/io/t4/e1.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java x1/c.java
00089	Connect to a URL and receive input stream from the server	command network	app/tango/o/setHasTransientState.java com/bumptech/glide/load/data/j.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java v6/c.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00109	Connect to a URL and get the response code	network command	app/tango/o/setHasTransientState.java com/bumptech/glide/load/data/j.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java v6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/lighthouse1/mobilebenefits/view/BottomNavigation.java com/samsung/android/sdk/samsungpay/v2/SamsungPay.java com/samsung/android/sdk/samsungpay/v2/WatchManager.java com/visa/mobileEnablement/pushProvisioning/p/b.java q3/k0.java w9/v.java
00036	Get resource file from res/raw directory	reflection	com/lighthouse1/mobilebenefits/view/BottomNavigation.java
00125	Check if the given file path exist	file	com/lighthouse1/mobilebenefits/activity/ScreenActivity.java com/lighthouse1/mobilebenefits/fragment/ScreenBaseFragment.java
00054	Install other APKs from file	reflection	w9/v.java
00026	Method reflection	reflection	bd/a.java bd/b.java
00114	Create a secure socket connection to the proxy address	network command	sdk/pendo/io/b3/f.java tf/f.java
00042	Query WiFi BSSID and scan results	collection wifi	com/lexisnexisrisk/threatmetrix/rl/tmxprofiling/vvcvccv.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/i.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	ab/b.java
00038	Query the phone number	collection	ab/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00067	Query the IMSI number	collection	ab/b.java
00082	Get the current WiFi MAC address	collection wifi	ab/b.java
00096	Connect to a URL and set request method	command network	app/tango/o/setHasTransientState.java v6/c.java
00012	Read data and put it into a buffer stream	file	sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java
00014	Read file into a stream and put it into a JSON object	file	u6/c.java
00094	Connect to a URL and read data from it	command network	external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.CAMERA, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.ACCESS_LOCATION_EXTRA_COMMANDS, android.permission.BLUETOOTH

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
mws.navigatorsuite.com	ok	**IP:** 45.223.161.93 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.eu.pendo.io	ok	**IP:** 34.110.214.126 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.pendo-uat.pendo-dev.com	ok	**IP:** 34.120.16.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.k006bk006bk006bk	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.hh00680068h00680068z10	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
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.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
www.h0068hhh00680068	ok	No Geolocation information available.
www.h006800680068h00680068hashmap	ok	No Geolocation information available.
data.jpn.pendo.io	ok	**IP:** 34.149.195.87 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
www.hh006800680068h0068i10	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.gstatic.com	ok	**IP:** 142.250.188.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
i1mws.evolution1.com	ok	**IP:** 45.223.161.93 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
data.pendo.io	ok	**IP:** 34.107.204.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.h0068h00680068h0068	ok	No Geolocation information available.
www.hh0068h0068h0068	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
us1.data.pendo.io	ok	**IP:** 34.110.177.118 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
test@example.com customerservice@wexhealth.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Pendo	Analytics	https://reports.exodus-privacy.eu.org/trackers/416

HARDCODED SECRETS

POSSIBLE SECRETS
"AuthorizationServicesTokensElevatePermissionsUriQueryString" : "?ElevatePermissions=true"
"AuthorizationServicesTokensUriPathSegment" : "/Tokens/"
"CredentialType" : "RsaIdpNative"
"PendoAPIKey" : "eyJhbGciOiJSUzI1NiIsImtpZCI6IiIsInR5cCI6IkpXVCJ9.eyJkYXRhY2VudGVyIjoidXMiLCJrZXkiOiJlYjVmYzZhN2E1ZjBiOWIyMTZlY2FkNTE5MzIzMDBlOGQ4ZDE5NDhhYjkyY2NjNGFhMTZlZmM0YjNjOTFiMDM2MTdjNjQ0MzE2M2FkZGQ2ZWVlMGQ1ZWExZmZjMjU2MDY1Nzg2ZjMyYjkwOGU3NmE1ZGI5NDVhY2YwNzJjODIwMzRjN2U2YjkxODFkODU5MDYzYzc2MzYyMmJjNzQ2OTcwMGI5YWUyOGJiNjQyNzUxOGRmZTZlMWE0NDMxYjI1ODc0MGUyNDUwZGVkZDMwOGJhODliYzk5Mjc2MjJmOTQzZS5hNTU3ZGYyMjdmZmRlOWM2NTg0YWM0YWZkMTlmNjc4YS5mNzkzZTE5MzJkYzc4YTA3YTM1Y2JjN2NhM2U2YzMwMmRhZjlkNDEwNTBlYmI4Y2EwNWViZDBhMDM5MmMxNGM1In0.LyMfYO_FdFSUzCXjKsuj5HPeS6yiw-50bYNfNy8NwJ_pxIunWxLwbKbqygsWE6Bd1AIH2SA9mEMbRJij8GeYbfGx1FvrbFvziSLtlgo4QJcdxca3ll21eog3jvrxCWb82XqG83vMCln9L85F5RNXpybUygi2dgbLkYGkXUYq6u0"
"appauthtoken_reauthorize" : "Reauthorize"
"login_password" : "Password"
"login_username" : "Username"
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1B6qsa2sbpc4CuFEjgRWez9nN

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
410583637251521421293261297800472684091144410159937255548352563140394674012 91
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
VTdL1VbC2tejvcI2BlMkEpk1BzBZI0KQB0GaDWFLN
7fmduHKTdHHrlMvldlEqAIlSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
Vd99BKh6pxt3mXSDJzHuVrCq52xBXAKVahbuFb6dqBc
32670510020758816978083085130507043184471273380659243275938904335757337482424
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1QIw
nvknbo5+6pBVWVZpCg5Rtpii3JUKMxOmJrccBCo7ICIqPIj/L9Nc5zmWMH2igKHLq
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
55066263022277343669578718895168534326250603453777594175500187360389116729240
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF
9c6b87fd-4bfa-4e46-a244-ef1e213bc64a
115792089237316195423570985008687907852837564279074904382605163141518161494337
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573530086143415290314195533631308867097853951
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
05e3f287-4cb8-4706-b157-ffc01942fed0

POSSIBLE SECRETS
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
94da5232-8d8e-46e1-b851-9cb80141c59d
115792089210356248762697446949407573529996955224135760342422259061068512044369
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

POSSIBLE SECRETS
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
962eddcc369cba8ebb260ee6b6a126d9346e38c5
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
115792089210356248762697446949407573530086143415290314195533631308867097853948
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF
115792089237316195423570985008687907853269984665640564039457584007908834671663

POSSIBLE SECRETS
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 48
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
34df0e7a9f1cf1892e45c056b4973cd81ccf148a4050d11aea4ac5a65f900a42
sXchDaQebHnPiGvyDOAT4saGEUetSyo9MKLOoWFsueri23bOdgWp4Dy1WlUzewbgBHod5pcM9H95GQRV3JDXboIRROSBigeC5yjU1hGzHHyXss8UDprecbAYxknTcQkhslANGRUZmdTOQ5qTRsLAt6BTYuyvVRdhS8exSZEy
FDB497E7C6F9D71A89D042B0FA5B7A4DEA5EE7938F08CFDA9F1FB58EBDF749E7

POSSIBLE SECRETS
48439561293906451759052585252797914202762949526041747995844080717082404635286
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
9760508f15230bccb292b982a2eb840bf0581cf5
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
473222bd-48e8-4900-8997-7882b1b5071c
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbelsiqvdpzGmRF3pex4Ar1HNI

POSSIBLE SECRETS
UhbMtiAExFNPNceArXxYL07lKDceJ9QVHwVTMl3pzL5rNOxCM
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
Ct4eTlXHBIY2EaV7t7LjJaynVJCpkv4LKjTTAumiGUIuQhrNhZLuF
57896044618658097711785492504343953926634992332820282019728792003956564819949
8d5155894229d5e689ee01e6018a237e2cae64cd
7268387242956068905493238078880045343536413606873180602814901991806123281667307726863963836986765459300888844618436373610534980183654 39
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCv8IqRRwpH8s7EnWhLwuFqnbTA
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

POSSIBLE SECRETS
nMcadFr9rwxGUMGOn8qIcjLE4vr9T1rxm6DekW9IBGNAwGOynuA+ebTfpfPMYY8nO

PLAYSTORE INFORMATION

Title: Benefits by WEX

Score: 3.643204 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.lighthouse1.mobilebenefits.dbi

Developer Details: WEX, Inc., WEX,+Inc., None, https://www.wexinc.com/contact/health, customerservice@wexhealth.com,

Release Date: Dec 9, 2010 **Privacy Policy:** Privacy link

Description:

Keep tabs on all your benefit accounts by quickly checking your balances and details using our secure mobile app. With real-time access and intuitive navigation to all your important account information, our app includes the following features: Easy, Convenient & Secure • Simply login to the intuitive app using your same health benefits website username and password (or follow alternative instructions if provided) • No sensitive account information is ever stored on your mobile device • Use Touch ID or Face ID to quickly log in to the mobile app Connects You with the Details • Quickly check available balances 24/7 • View charts summarizing account(s) • View claims requiring receipts • Click to call or email Customer Service • View your statements and notifications • Scan product barcodes to determine their eligibility Provides Additional Time-Saving Options (if supported or applicable to your account(s)) • File a claim towards your FSA and HRA • Take or upload a picture of a receipt and submit for a new or existing claim • View, contribute and distribute HSA transactions • Pay bills from any account and add a payee • Manage your expenses by entering medical expense information and supporting documentation • View and Manage your HSA investments • Retrieve your forgotten username/password • Report a debit card as lost or stolen Powered by WEX Health®

SCAN LOGS

Timestamp	Event	Error
2025-08-31 01:00:25	Generating Hashes	OK

2025-08-31 01:00:25	Extracting APK	OK
2025-08-31 01:00:25	Unzipping	OK
2025-08-31 01:00:25	Parsing APK with androguard	OK
2025-08-31 01:00:25	Extracting APK features using aapt/aapt2	OK
2025-08-31 01:00:26	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 01:00:28	Parsing AndroidManifest.xml	OK
2025-08-31 01:00:28	Extracting Manifest Data	OK
2025-08-31 01:00:28	Manifest Analysis Started	OK
2025-08-31 01:00:28	Reading Network Security config from network_security_config.xml	OK
2025-08-31 01:00:28	Parsing Network Security config	OK
2025-08-31 01:00:28	Performing Static Analysis on: Benefits (com.lighthouse1.mobilebenefits.dbi)	OK

2025-08-31 01:00:29	Fetching Details from Play Store: com.lighthouse1.mobilebenefits.dbi	OK
2025-08-31 01:00:32	Checking for Malware Permissions	OK
2025-08-31 01:00:32	Fetching icon path	OK
2025-08-31 01:00:32	Library Binary Analysis Started	OK
2025-08-31 01:00:32	Reading Code Signing Certificate	OK
2025-08-31 01:00:34	Running APKiD 2.1.5	OK
2025-08-31 01:00:38	Detecting Trackers	OK
2025-08-31 01:00:40	Decompiling APK to Java with JADX	OK
2025-08-31 01:15:57	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-31 01:15:57	Decompiling classes2.dex with JADX	OK
2025-08-31 01:16:12	Decompiling classes.dex with JADX	OK

2025-08-31 01:16:12	Decompiling classes2.dex with JADX	OK
2025-08-31 01:16:27	Decompiling classes.dex with JADX	OK
2025-08-31 01:16:39	Converting DEX to Smali	OK
2025-08-31 01:16:39	Code Analysis Started on - java_source	OK
2025-08-31 01:16:44	Android SBOM Analysis Completed	OK
2025-08-31 01:16:56	Android SAST Completed	OK
2025-08-31 01:16:56	Android API Analysis Started	OK
2025-08-31 01:17:06	Android API Analysis Completed	OK
2025-08-31 01:17:08	Android Permission Mapping Started	OK
2025-08-31 01:17:16	Android Permission Mapping Completed	OK
2025-08-31 01:17:17	Android Behaviour Analysis Started	OK

2025-08-31 01:17:32	Android Behaviour Analysis Completed	OK
2025-08-31 01:17:32	Extracting Emails and URLs from Source Code	OK
2025-08-31 01:17:38	Email and URL Extraction Completed	OK
2025-08-31 01:17:38	Extracting String data from APK	OK
2025-08-31 01:17:38	Extracting String data from Code	OK
2025-08-31 01:17:38	Extracting String values and entropies from Code	OK
2025-08-31 01:17:41	Performing Malware check on extracted domains	OK
2025-08-31 01:17:45	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.