ANDROID STATIC ANALYSIS REPORT

app_icon

Optum Perks (2.1.0 (2023111601))

File Name:	com.optum.mobile.perks_2023111601.apk
Package Name:	com.optum.mobile.perks
Scan Date:	Sept. 1, 2025, 6:46 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	17	4	2	1

FILE INFORMATION

File Name: com.optum.mobile.perks_2023111601.apk
Size: 8.13MB
MD5: 7bfb7867783c85147121ebb113ed29e0
SHA1: ead384eed5a855bdb74f611b19cdff78d012de85
SHA256: 5ae70c7d7e451aa30e0f5a567ea5e77aafafb3373650d14249078d8afc4096ea

APP INFORMATION

App Name: Optum Perks
Package Name: com.optum.mobile.perks
Main Activity: androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity
Target SDK: 34
Min SDK: 23

Max SDK:

Android Version Name: 2.1.0 (2023111601)

Android Version Code: 2023111601

APP COMPONENTS

Activities: 32

Services: 5

Receivers: 4

Providers: 2

Exported Activities: 5

Exported Services: 0

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=MN, L=Minnetonka, O=UnitedHealth Group, OU=OptumHealth, CN=OptumHealth

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2011-02-21 20:24:53+00:00

Valid To: 2038-07-09 20:24:53+00:00

Issuer: C=US, ST=MN, L=Minnetonka, O=UnitedHealth Group, OU=OptumHealth, CN=OptumHealth

Serial Number: 0x4d62ca15

Hash Algorithm: sha1

md5: e60b15959bd0153f1dc8ec05a0c3c3a3

sha1: 497ebf0012b712bda799ef1e9cca6cdbf3b2e919

sha256: 987a7c6c4d21181de15674508b0d8724d0bc5884dafc081ba06872f2207485a5

sha512: 3f85b1feda16703a2de15579789f624718369c4a3d2e5984ee795d6d78711e716031af24a806c7828e93bbc94277fd28599d955a58a6532c204b977bd0f9c421

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 11d7e0be4d679f8ad09a24d57477726379c34890e55964e5213bf457350b2ae5
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.optum.mobile.perks.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

<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.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name 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>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.optum.mobile.perks.ui.start.StartActivity	Schemes: https://, Hosts: optumperks-alternate.app.link,
com.optum.mobile.perks.Launcher	Schemes: https://, optumperks://, Hosts: perks.optum.com, Path Patterns: /coupon/.*,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **2** | 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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.optum.mobile.perks.ui.start.StartActivity) 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
3	App Link assetlinks.json file not found [android:name=com.optum.mobile.perks.Launcher] [android:host=https://perks.optum.com]	high	App Link asset verification URL (https://perks.optum.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 403). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	Activity-Alias (com.optum.mobile.perks.Launcher) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	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.
6	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
7	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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	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: **6** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/p.java a4/c.java aa/b.java aj/k.java b3/m.java b5/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b7/d.java b7/f.java ba/c.java bd/d.java c3/f.java c3/g.java c3/h.java c3/i.java c3/j.java c5/c.java c9/a.java c9/c.java c9/d.java cj/j.java cj/l.java com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/AnalyticsExtension.java com/adobe/marketing/mobile/AnalyticsHitsDatabase.java com/adobe/marketing/mobile/AnalyticsListenerAcquisitionResponseContent.java com/adobe/marketing/mobile/AnalyticsListenerAnalyticsRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerConfigurationResponseContent.java com/adobe/marketing/mobile/AnalyticsListenerGenericTrackRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerHubSharedState.java com/adobe/marketing/mobile/AnalyticsListenerRulesEngineResponseContent.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidDatabase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/AndroidDatabaseService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/AndroidJsonUtility.java com/adobe/marketing/mobile/AndroidLoggingService.java com/adobe/marketing/mobile/AndroidNetworkService.java com/adobe/marketing/mobile/AndroidSystemInfoService.java com/adobe/marketing/mobile/AndroidUIService.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/ConfigurationListenerRequestContent.java com/adobe/marketing/mobile/ContextDataUtil.java com/adobe/marketing/mobile/Core.java com/adobe/marketing/mobile/Event.java com/adobe/marketing/mobile/EventDataFlattener.java com/adobe/marketing/mobile/EventHub.java com/adobe/marketing/mobile/ExtensionApi.java com/adobe/marketing/mobile/FileUtil.java com/adobe/marketing/mobile/HitQueue.java com/adobe/marketing/mobile/IdentityExtension.java com/adobe/marketing/mobile/LegacyStaticMethods.java com/adobe/marketing/mobile/LifecycleExtension.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/MobileCore.java com/adobe/marketing/mobile/MobileServicesExtension.java com/adobe/marketing/mobile/MobileServicesPlatform.java com/adobe/marketing/mobile/PersistentProfileData.java com/adobe/marketing/mobile/RangedResolver.java com/adobe/marketing/mobile/RemoteDownloader.java com/adobe/marketing/mobile/RuleCondition.java com/adobe/marketing/mobile/RulesRemoteDownloader.java com/adobe/marketing/mobile/SignalExtension.java com/adobe/marketing/mobile/SignalHitsDatabase.java com/adobe/marketing/mobile/TargetExtension.java com/adobe/marketing/mobile/TargetListenerRequestContent.java com/adobe/marketing/mobile/TargetOrder.java com/adobe/marketing/mobile/TargetParameters.java com/adobe/marketing/mobile/TargetRequestBuilder.java com/adobe/marketing/mobile/TimerState.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/b.java com/bumptech/glide/d.java com/bumptech/glide/e.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/l.java com/bumptech/glide/manager/n.java com/bumptech/glide/manager/t.java com/bumptech/glide/manager/u.java com/bumptech/glide/manager/w.java com/bumptech/glide/o.java com/bumptech/glide/q.java d3/d.java d5/b0.java d5/j0.java d5/m.java d5/n.java d5/r.java d9/r.java de/x.java dg/d.java dj/b.java e0/f1.java e5/h.java e5/i.java f/c0.java f/d0.java f/h0.java f/j.java f4/b.java f4/e.java f4/f.java fi/g.java g4/b.java g4/b0.java g4/o.java g4/p.java g7/k.java gb/a.java gb/b.java h3/p.java h5/c0.java h5/e0.java h5/g.java h5/i.java h5/k.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	h5/w.java h6/b.java hb/g.java i3/a.java i4/c.java i4/e.java i6/d.java i6/k.java j0/u1.java j5/b.java j7/j.java ja/e.java jf/b.java k/i.java k/j.java k2/p.java k5/b.java k5/b0.java k5/c.java k5/h0.java k5/i.java k5/n.java k5/s.java k5/x.java k8/c.java kj/m.java l/h.java l/j.java l/p.java l2/d.java l8/c.java l9/a.java l9/d.java l9/g.java lj/d.java m5/a.java m5/b.java m5/h.java m5/k.java ma/c.java n2/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n2/e.java n2/m.java n3/c.java n3/c2.java n3/d2.java n3/f1.java n3/h2.java n3/i1.java n3/t0.java n3/y.java n8/d.java na/b.java o1/u0.java o8/a.java oa/c.java og/s.java p7/j.java p9/a.java p9/d.java p9/h.java q2/g.java q5/i.java q6/b.java q6/c.java q6/d.java q6/f.java q6/g.java q6/i.java q6/k.java q8/e.java q8/h.java q9/a.java q9/d.java qa/a0.java qa/b0.java qa/c0.java qa/e.java qa/e0.java qa/g.java qa/g0.java qa/h.java qa/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				qa/i.java qa/j.java qa/l.java qa/n.java qa/u.java qa/v.java qa/w.java qa/x.java qi/x.java r3/v.java r4/c.java r5/f.java r6/e.java r6/i.java r6/j.java r6/m.java r6/o.java r6/s.java r9/b.java r9/c.java re/k.java s0/l.java s2/e.java s2/j.java s2/o.java s2/p.java s3/c.java s7/a.java sa/b.java sb/b1.java t2/a0.java t2/c0.java t2/d.java t2/f.java t2/f0.java t2/g.java t2/i.java t2/k.java t2/m.java t2/n.java t2/p.java t2/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t2/t.java t6/e.java t6/f0.java t6/s.java t6/u.java t6/w.java t7/a.java t9/b.java u2/a.java u2/b.java u2/d.java u2/g.java u2/h.java u2/j.java u2/n.java u2/u.java u5/b.java u6/c0.java u6/e0.java u6/f.java u6/g.java u6/n.java u6/q.java u6/w.java u6/x.java u6/z.java u9/e.java u9/g.java u9/h.java u9/j.java u9/l.java u9/n.java u9/o.java u9/p.java u9/q.java u9/r.java u9/t.java u9/u.java u9/w.java v0/e.java v3/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v9/b.java v9/e.java v9/j.java v9/k.java w2/g.java w4/a0.java w4/h.java w7/c.java wa/a.java x0/d.java x4/c.java x4/d.java x6/a.java xa/d.java y2/c1.java y2/i.java y3/b.java y3/c.java y3/g.java y4/d.java y4/e.java y6/b.java ye/b2.java z/k0.java z1/d0.java z1/n.java z6/a.java z9/a.java z9/b.java
2	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	na/b.java u9/e.java z9/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	cb/d.java gb/i.java hb/f.java j$/util/concurrent/ThreadLocalRandom.java ji/a.java ji/b.java ki/a.java p9/g.java z1/n.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	kj/e.java kj/h.java kj/l.java kj/m.java
5	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	f4/e.java r9/c.java
6	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	b5/m.java d5/f.java d5/h0.java d5/z.java g0/b1.java j0/d1.java lc/d.java lc/e.java y1/n.java y1/s0.java yi/l0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	a1/e.java com/adobe/marketing/mobile/AndroidDatabase.java h6/b.java i6/d.java i6/j.java i6/k.java j6/e.java j6/h.java j6/i.java j6/o.java p9/a.java sb/n1.java sb/t.java
8	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/adobe/marketing/mobile/LegacyRemoteDownload.java
9	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	z6/a.java
10	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	com/optum/mobile/perks/ui/coupon/CouponDetailsActivity.java com/optum/mobile/perks/ui/coupon/PharmacyDetailsActivity.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	u9/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	sb/b1.java uc/f.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ag/a.java aj/k.java b5/j.java com/adobe/marketing/mobile/AndroidUIService.java com/adobe/marketing/mobile/LegacyMessageAlert.java com/adobe/marketing/mobile/LegacyMessageFullScreen.java com/adobe/marketing/mobile/LegacyMessageOpenURL.java com/adobe/marketing/mobile/LegacyReferrerHandler.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/MessageNotificationHandler.java com/bumptech/glide/e.java com/iterable/iterableapi/IterableFirebaseMessagingService.java com/optum/mobile/perks/ui/coupon/CouponDetailsActivity.java com/optum/mobile/perks/ui/coupon/PharmacyDetailsActivity.java df/f0.java g4/a.java g4/b.java mf/e.java og/c.java r6/f.java sb/w1.java u9/g.java
00036	Get resource file from res/raw directory	reflection	ag/a.java aj/k.java b5/j.java com/adobe/marketing/mobile/MessageNotificationHandler.java com/bumptech/glide/e.java com/iterable/iterableapi/IterableFirebaseMessagingService.java g4/a.java og/c.java r6/f.java u9/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	ba/c.java com/bumptech/glide/e.java e0/f1.java r9/c.java v9/e.java
00013	Read file and put it into a stream	file	b5/g.java ba/c.java c3/h.java c3/i.java cj/j.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/FileUtil.java com/adobe/marketing/mobile/LegacyMobileConfig.java com/bumptech/glide/d.java com/bumptech/glide/e.java d3/d.java e0/f1.java k4/b.java k4/i.java r9/c.java u9/e.java v9/e.java v9/k.java x4/d.java x4/f.java y3/g.java z6/a.java z9/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/marketing/mobile/LegacyRemoteDownload.java com/adobe/marketing/mobile/LegacyThirdPartyQueue.java com/adobe/marketing/mobile/MobileServicesExtension.java com/bumptech/glide/load/data/l.java f4/e.java oa/c.java og/a.java og/n.java p9/a.java sb/j1.java
00030	Connect to the remote server through the given URL	network	com/adobe/marketing/mobile/LegacyRemoteDownload.java com/bumptech/glide/load/data/l.java og/n.java
00109	Connect to a URL and get the response code	network command	com/adobe/marketing/mobile/LegacyRemoteDownload.java com/adobe/marketing/mobile/MobileServicesExtension.java com/bumptech/glide/load/data/l.java f4/e.java oa/c.java og/a.java og/n.java p9/a.java sb/j1.java
00022	Open a file from given absolute path of the file	file	com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/HitQueue.java com/adobe/marketing/mobile/LegacyAbstractDatabaseBacking.java com/adobe/marketing/mobile/LegacyRemoteDownload.java com/adobe/marketing/mobile/RemoteDownloader.java f4/e.java v9/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/adobe/marketing/mobile/LegacyThirdPartyQueue.java og/a.java og/n.java p9/a.java sb/j1.java
00094	Connect to a URL and read data from it	command network	com/adobe/marketing/mobile/LegacyRemoteDownload.java com/adobe/marketing/mobile/LegacyThirdPartyQueue.java com/adobe/marketing/mobile/MobileServicesExtension.java f4/e.java og/n.java u9/g.java
00108	Read the input stream from given URL	network command	com/adobe/marketing/mobile/LegacyRemoteDownload.java com/adobe/marketing/mobile/LegacyThirdPartyQueue.java com/adobe/marketing/mobile/MobileServicesExtension.java f4/e.java og/n.java
00114	Create a secure socket connection to the proxy address	network command	gj/l.java
00091	Retrieve data from broadcast	collection	com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/MessageNotificationHandler.java com/iterable/iterableapi/ui/inbox/IterableInboxActivity.java d9/r.java e0/f1.java og/c.java qa/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	aj/k.java com/adobe/marketing/mobile/AndroidUIService.java com/adobe/marketing/mobile/LegacyMessageAlert.java com/adobe/marketing/mobile/LegacyMessageFullScreen.java com/adobe/marketing/mobile/LegacyMessageOpenURL.java com/adobe/marketing/mobile/LegacyReferrerHandler.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/MessageNotificationHandler.java com/bumptech/glide/e.java com/optum/mobile/perks/ui/coupon/CouponDetailsActivity.java com/optum/mobile/perks/ui/coupon/PharmacyDetailsActivity.java g4/a.java g4/b.java og/c.java r6/f.java u9/g.java
00012	Read data and put it into a buffer stream	file	y3/g.java
00189	Get the content of a SMS message	sms	b7/d.java
00188	Get the address of a SMS message	sms	b7/d.java
00200	Query data from the contact list	collection contact	b7/d.java
00201	Query data from the call log	collection calllog	b7/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	b7/d.java
00072	Write HTTP input stream into a file	command network file	com/adobe/marketing/mobile/LegacyRemoteDownload.java f4/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/adobe/marketing/mobile/LegacyRemoteDownload.java kj/d.java kj/m.java u4/c.java
00004	Get filename and put it to JSON object	file collection	com/bumptech/glide/e.java e0/f1.java qi/x.java
00162	Create InetSocketAddress object and connecting to it	socket	kj/d.java kj/m.java
00016	Get location info of the device and put it to JSON object	location collection	e0/f1.java
00104	Check if the given path is directory	file	com/bumptech/glide/f.java
00075	Get location of the device	collection location	f/j.java
00137	Get last known location of the device	location collection	f/j.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/AndroidSystemInfoService.java com/adobe/marketing/mobile/LegacyStaticMethods.java
00005	Get absolute path of file and put it to JSON object	file	v9/e.java
00202	Make a phone call	control	com/optum/mobile/perks/ui/coupon/PharmacyDetailsActivity.java
00203	Put a phone number into an intent	control	com/optum/mobile/perks/ui/coupon/PharmacyDetailsActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/bumptech/glide/d.java p9/a.java
00026	Method reflection	reflection	qi/x.java
00009	Put data in cursor to JSON object	file	sb/n1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://optum-perks.firebaseio.com

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, 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
pay.google.com	ok	**IP:** 64.233.161.92 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.eu.iterable.com	ok	**IP:** 34.254.102.241 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
perks.optum.com	ok	**IP:** 172.200.65.176 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
images.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.179.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.perks.optum.com	ok	**IP:** 172.200.65.176 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aep-sdks.gitbook.io	ok	**IP:** 172.64.147.209 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
nullpointer.wtf	ok	No Geolocation information available.
api-prf.perks.optum.com	ok	**IP:** 20.36.188.227 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
optum-perks-mock-api.livefront.com	ok	**IP:** 99.83.220.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
livefront.com	ok	**IP:** 3.171.100.95 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
example.com	ok	**IP:** 23.192.228.84 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
store.optum.com	ok	**IP:** 15.197.167.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
login.microsoftonline.com	ok	**IP:** 20.190.190.132 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.iterable.com	ok	**IP:** 34.197.231.174 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
safety.google	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.link	ok	**IP:** 18.238.109.28 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
optum-perks.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
api2.branch.io	ok	**IP:** 18.238.96.83 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.38.161.73 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
api-dev.perks.optum.com	ok	**IP:** 172.200.60.79 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

✉ EMAILS

EMAIL	FILE
joe.cool@optum.com	le/c0.java
u0013android@android.com0 u0013android@android.com	r6/q.java

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"account_information_password" : "Password"
"com.google.firebase.crashlytics.mapping_file_id" : "e0e1cd3f9f2849d48421e18d4dfa01f6"
"firebase_database_url" : "https://optum-perks.firebaseio.com"
"library_colocation_authorWebsite" : "https://nullpointer.wtf"
d0f80cf0-6c3a-40bf-b025-3213685e9acf
470fa2b4ae81cd56ecbcda9735803434cec591fa
AIzaSyBebfGKDwLRMa8368OO4Zr7RwvFuxSjU40
2e81d682-a63f-4f2e-8c26-097a2f02cf63
5a558cc3-2843-4996-9cc8-35f1dd274d6b

POSSIBLE SECRETS
eyJpc3MiOiJhYXJwLXBheS1zZXJ2aWNlLWFjY291bnRAYWFycC1waGFybWFjeS5pYW0uZ3NlcnZpY2VhY2NvdW50LmNvbSIsImF1ZCI6Imdvb2dsZSIsInR5cCI6InNhdmV0b2FuZHJvaWRwYXkiLCJpYXQiOjE2NDM5MTc3MDksInBheWxvYWQiOnsibG95YWx0eU9iamVjdHMiOlt7ImJhcmNvZGUiOnsidHlwZSI6InFyQ29kZSIsInZhbHVlIjoiZTVkOTNjMWYtYTU2ZS00NGJhLWExY2YtZDM2NDEwOWU3ZjhjIn0sImNsYXNzSWQiOiIzMzg4MDAwMDAwMDIxOTk2NDgwLkNPVVBPTl9DTEFTU19lNWQ5M2MxZi1hNTZlLTQ0YmEtYTFjZi1kMzY0MTA5ZTdmOGNfMTg5M2Y3MTAtYWIxNi00YTNmLWFlYzgtOTY4YmJkMTNjZWIxIiwiaWQiOiIzMzg4MDAwMDAwMDIxOTk2NDgwLkNPVVBPTl9PQkpFQ1RfZTVkOTNjMWYtYTU2ZS00NGJhLWExY2YtZDM2NDEwOWU3ZjhjX2I0ZWFhNDNlLTg0ZTgtNDA3Ny04YjI4LTI5MDE4ZGM4ZTcwMCIsInN0YXRlIjoiYWN0aXZlIn1dfSwib3JpZ2lucyI6WyJodHRwczovL3BlcmtzLm9wdHVtLmNvbSJdLCJzY29wZXMiOlsiaHR0cHM6Ly93d3cuZ29vZ2xlYXBpcy5jb20vYXV0aC93YWxsZXRfb2JqZWN0Lmlzc3VlciJdfQ
d689b526-1aae-46ea-bc98-7960779428d4
d09aabf0-e7e3-4260-8850-f9f3154277c1
6da32084-0bca-4727-ab87-cb040b4fddd7
d43dba333d404d28bf325ae5b194906f
db05faca-c82a-4b9d-b9c5-0f64b6755421
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
00816c85-c4db-4b26-95d3-5f832fc71c39
C8ohqOwOO42E5Cckqw88Usszw9s13uJTvuOPFllU3ox8wMs5g
jic6JcL4M25eXXFhNPB988lEwFFafI7CzzOQPX2obn9feadGtUUMTnXG1iRfO0UlQlrrLfqOdVmNtuHEAe
TldKGNtbvOgRV37usfp0azlF
AIzaSyBk4v5GNB4CmLWTWBefYvfl6kET8FB8M5c

POSSIBLE SECRETS
mKfmBWPC35jAs6y0WYteTqtd2cCzQpzeR9B
3aad3e05-fddf-4477-b6da-bca577fd5325
f28f7bfe-efd5-44dc-9b37-3ae889ff31b2
urlVjhdasq3N7P5jqbcxRlzv8NbqxMlej8sLtjkxG
e571444d-1c52-4283-9186-b5e14d6aead1
eaa4c418-1acc-480c-aa97-981002b240fd
6b12c694-b09a-4627-a0b1-2ffae2d75988

PLAYSTORE INFORMATION

Title: Optum Perks: Rx Discount Card

Score: 4.6788993 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.optum.mobile.perks

Developer Details: Optum Inc., Optum+Inc., None, https://perks.optum.com/mobile-app, perks_support@optum.com,

Release Date: Sep 17, 2020 **Privacy Policy:** Privacy link

Description:

Say no to high prescription costs. Compare local pharmacies for the best prices and get free rx coupons to save you even more! Optum Perks is a brand dedicated to delivering real prescription discounts to those who need them the most. Our 100% free coupons can help you get major discounts on all FDA approved medication nationwide. It's as easy as searching for your prescription, finding the location nearest you with the best price, and going to pick up your prescription. Save hundreds on your medication costs, regardless of coverage status. Even if you have insurance or Medicare, Optum Perks may be able to beat your copay prices. Your health and well-being are incredibly important, but maintaining a healthy lifestyle doesn’t have to be expensive. As the top prescription discount app, Optum Perks has partnerships with pharmacies nationwide. Whether you are looking for a refill or picking up a prescription for the first time, Optum Perks can connect you with a pharmacist who can save you money. It’s super simple and 100% free to use: - Look up your prescription - Compare prices at local pharmacies - Get our free drug coupon right in the app - Show coupon to pharmacist and save instantly We’ve helped people save over $1 billion on their prescription costs. Put our savings in your pocket! Download Optum Perks for your next pharmacy visit. Optum Perks Features: Health Savings - Big savings on hundreds of medications - Participating pharmacies include: Walmart, CVS, Walgreens, Meijer, Genoa Healthcare, independent pharmacies and more - Price Comparison - Compare prices from different pharmacies to get the best deal Rx discounts from Optum Perks are used by hundreds of doctors and clinics to help save consumers’ money on their medications. By using Optum Perks, you agree to our terms and conditions. Read more on perks.optum.com/privacy-policy."

SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:46:11	Generating Hashes	OK
2025-09-01 06:46:11	Extracting APK	OK
2025-09-01 06:46:11	Unzipping	OK
2025-09-01 06:46:12	Parsing APK with androguard	OK
2025-09-01 06:46:12	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:46:12	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:46:15	Parsing AndroidManifest.xml	OK

2025-09-01 06:46:15	Extracting Manifest Data	OK
2025-09-01 06:46:15	Manifest Analysis Started	OK
2025-09-01 06:46:16	Performing Static Analysis on: Optum Perks (com.optum.mobile.perks)	OK
2025-09-01 06:46:17	Fetching Details from Play Store: com.optum.mobile.perks	OK
2025-09-01 06:46:19	Checking for Malware Permissions	OK
2025-09-01 06:46:19	Fetching icon path	OK
2025-09-01 06:46:19	Library Binary Analysis Started	OK
2025-09-01 06:46:19	Reading Code Signing Certificate	OK
2025-09-01 06:46:19	Running APKiD 2.1.5	OK
2025-09-01 06:46:22	Detecting Trackers	OK

2025-09-01 06:46:23	Decompiling APK to Java with JADX	OK
2025-09-01 06:46:36	Converting DEX to Smali	OK
2025-09-01 06:46:36	Code Analysis Started on - java_source	OK
2025-09-01 06:46:39	Android SBOM Analysis Completed	OK
2025-09-01 06:46:49	Android SAST Completed	OK
2025-09-01 06:46:49	Android API Analysis Started	OK
2025-09-01 06:46:58	Android API Analysis Completed	OK
2025-09-01 06:46:58	Android Permission Mapping Started	OK
2025-09-01 06:47:05	Android Permission Mapping Completed	OK
2025-09-01 06:47:06	Android Behaviour Analysis Started	OK
2025-09-01 06:47:17	Android Behaviour Analysis Completed	OK

2025-09-01 06:47:17	Extracting Emails and URLs from Source Code	OK
2025-09-01 06:47:21	Email and URL Extraction Completed	OK
2025-09-01 06:47:21	Extracting String data from APK	OK
2025-09-01 06:47:21	Extracting String data from Code	OK
2025-09-01 06:47:21	Extracting String values and entropies from Code	OK
2025-09-01 06:47:23	Performing Malware check on extracted domains	OK
2025-09-01 06:47:26	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.