ANDROID STATIC ANALYSIS REPORT

app_icon

myPrivia (2.32.0)

File Name:	com.priviamedicalgroup.priviaapp_972.apk
Package Name:	com.priviamedicalgroup.priviaapp
Scan Date:	Sept. 1, 2025, 7:54 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	24	4	3	1

FILE INFORMATION

File Name: com.priviamedicalgroup.priviaapp_972.apk
Size: 15.66MB
MD5: 130fea1b9b803efc7c8b0b1169aa621e
SHA1: 27b5b2e45f81dbacc6915a09e4dcac0d5645c615
SHA256: 54ff9890e2bb4b7c5b09b2eb38cf74fa955f8b4e5a56e221dd4a6ee759d5affc

APP INFORMATION

App Name: myPrivia
Package Name: com.priviamedicalgroup.priviaapp
Main Activity: com.priviamedicalgroup.priviaapp.ui.welcomeView.presentation.view.SplashActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 2.32.0

Android Version Code: 972

APP COMPONENTS

Activities: 16
Services: 18
Receivers: 17
Providers: 3
Exported Activities: 6
Exported Services: 1
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-04-10 16:54:51+00:00
Valid To: 2048-04-10 16:54:51+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x676b10b769b5bdfb339fe5a72527945825fcded6
Hash Algorithm: sha256
md5: 3a91cb703da45b03c5db819d9d612383
sha1: 3bfdf09e6830927d293fe6d737c3c6eb4699724b
sha256: 60506fd08da3bf731920edc956f7fc4cb1f6b381d2fdd774063a87e1874a20c4
sha512: 82394a0356efac7367fa9249b1175a4930e5f0404587d234a4fc76cd73a03d40004451d9bda5187e5cbccd0a609adab81bb9d06f1bf49c6f92cddcf9c0e6eb9d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: d593e7863ca4bd14bba900cbafcba01184e838d1162437ccbb6df2f376339be4
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.priviamedicalgroup.priviaapp.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
com.priviamedicalgroup.priviaapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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 ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.priviamedicalgroup.priviaapp.deep_link.PatientDeepLinkActivity	Schemes: myprivia://, https://, Hosts: stage2.priviahealth.com, rc.priviahealth.com, secure.priviahealth.com, shortbread.pt.priviahealth.com, privia.io, Path Prefixes: /virtual-visits/patients, /privia-virtual-health, /kr, /vv,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.priviamedicalgroup.priviaapp://,

🔒 NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	shortbread.pt.priviahealth.com fad.pt.priviamedicalgroup.com priviamedicalgroup.com myprivia.com priviahealth.com privia.io	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **15** | 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	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 (com.priviamedicalgroup.priviaapp.ui.athenaVideoCall.presentation.AthenaVideoCall) 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 (com.priviamedicalgroup.priviaapp.deep_link.PatientDeepLinkActivity) 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
5	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 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.
6	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) 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.
7	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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.
13	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
14	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
16	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.
17	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/f.java a1/i.java a5/b.java a6/b.java a6/c.java aa/a0.java aa/b0.java aa/c0.java aa/d0.java aa/e.java aa/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aa/g.java aa/g0.java aa/h.java aa/h0.java aa/j0.java aa/k.java aa/k0.java aa/l.java aa/o.java aa/p.java aa/q.java aa/r.java ai/k.java b1/d.java b1/e.java b1/f.java b1/g.java b1/h.java b1/m.java b5/d.java b5/e.java bi/d.java c7/a.java com/athenahealth/telehealth/ui/fragments/BaseFragment.java com/biba/bibacommon/ProxyConfig.java com/bugsnag/android/i1.java com/bumptech/glide/b.java com/bumptech/glide/h.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/SupportRequestManagerFragment.java com/onesignal/debug/internal/logging/a.java com/priviamedicalgroup/priviaapp/ui/messaging/presentation/view/SendMessagesFragment.java com/priviamedicalgroup/priviaapp/ui/tableSpace/presentation/TableSpacePickerActivity.java com/vidyo/lmi/BatteryManager.java com/vidyo/lmi/LocationManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/vidyo/lmi/LocationManager.java com/vidyo/lmi/ScreenManager.java com/vidyo/lmi/ui/Window.java com/xodee/client/audio/audioclient/AudioClient.java d2/d.java d5/a.java d6/b.java d7/b.java d7/i.java d7/j.java df/b.java e4/c.java e5/a0.java e5/j.java e5/k.java e5/m.java e5/r.java e8/a.java e9/e.java f1/f.java f1/l.java f3/j.java f3/n.java f3/p.java f5/h.java f5/i.java f9/a.java g/f.java g/g.java g/h.java g/r.java g/s.java g/t.java g0/b.java g2/h.java g2/i.java g2/j.java g2/o.java g2/p.java g5/d.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	g5/i.java g6/k.java h1/c.java h5/a.java h7/b.java i4/a.java i5/c.java i5/e.java i5/s.java j1/a.java j1/b.java j1/h0.java j1/k0.java j1/t.java j1/y0.java j4/c.java j6/a.java j9/a.java j9/j.java k0/b.java k2/c.java k6/b.java l/f.java l2/d.java l5/a0.java l5/c.java l5/h.java l5/j.java l5/l.java l5/m.java l5/q.java l5/x.java l6/d.java lc/c.java m2/a.java m6/q.java n1/k.java n8/c.java ne/y.java o1/b.java o4/a0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o4/c.java o4/f.java o4/g.java o4/j.java o4/k.java o4/l.java of/b0.java p0/d.java p5/a.java p5/i.java p7/m7.java p7/w2.java p7/y4.java p8/a.java q2/a.java q4/a.java q6/a.java q6/b.java r0/e.java r1/c.java r4/f.java r5/d.java r5/i.java r5/j.java r6/b.java r6/o.java r6/p.java r7/a.java s2/d.java s2/i.java s7/a.java s8/d.java t/c0.java t/l.java t/n.java t/t.java t/u0.java t0/d.java t4/b.java t4/c.java t4/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t4/e.java t4/f.java t4/g.java t4/h.java t8/a.java u0/a.java u0/b.java u5/g.java ue/b.java v2/k.java v2/m.java v5/d.java v5/i.java v6/b.java v6/c.java v6/f.java v6/i.java v6/p.java v6/q.java v6/s.java v6/v.java v6/w.java v7/g.java v9/d.java w1/a.java w2/c.java w2/e0.java w6/c0.java w6/e.java w6/f.java w6/j.java w6/k.java w6/l.java w6/t.java w6/x.java w8/f.java x/e.java x/k.java x9/b.java y0/d.java y0/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y0/k.java y0/u.java y1/b.java y6/d.java y6/d0.java y6/f0.java y6/h0.java y6/k0.java y6/m.java y6/s0.java y6/u0.java y6/z.java y9/c.java z/p0.java z/u0.java z0/b.java z5/a.java z6/b.java z6/e.java z6/g0.java z6/n0.java z6/r0.java z6/s.java z6/u.java z6/x0.java z6/y.java z6/z0.java ze/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	c5/g.java com/bugsnag/android/b1.java com/onesignal/core/internal/http/impl/d.java com/onesignal/inAppMessages/internal/prompt/impl/b.java com/onesignal/notifications/bridges/a.java com/onesignal/notifications/internal/c.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/priviamedicalgroup/priviaapp/network/model/Visit.java e3/d.java e5/f.java e5/q.java e5/x.java oc/a.java rc/e.java w4/e.java
3	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	a4/e.java b0/v1.java com/onesignal/session/internal/outcomes/impl/m.java l2/c.java m6/q.java m6/x.java p7/i.java p7/j.java p7/q2.java p7/s7.java ya/c.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	ai/d.java ai/e.java ai/j.java ai/k.java j4/c.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	com/onesignal/common/AndroidUtils.java f9/a.java ih/a.java ih/b.java jh/a.java p7/m7.java r6/f.java t/y.java
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	of/t.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java g/s.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	aa/o.java com/bugsnag/android/g0.java x9/b.java y9/c.java
9	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	com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java of/j.java x9/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	p7/m7.java
11	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	com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java of/j.java
12	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/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/onesignal/common/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	aa/e.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/priviamedicalgroup/priviaapp/deep_link/PatientDeepLinkActivity.java com/priviamedicalgroup/priviaapp/ui/appointment/presentation/view/AppointmentDetailsFragment.java com/priviamedicalgroup/priviaapp/ui/dashboard/presentation/view/fragment/DashboardFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/ContactUsFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/insurance/AddInsuranceFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/profile/ConsentToTreatFormFragment.java com/priviamedicalgroup/priviaapp/ui/welcomeView/presentation/view/QuickStartViewActivity.java ge/b.java ge/i1.java me/m.java me/w.java ob/b.java of/j.java p7/o5.java w6/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	aa/e.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/priviamedicalgroup/priviaapp/deep_link/PatientDeepLinkActivity.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java com/priviamedicalgroup/priviaapp/ui/welcomeView/presentation/view/QuickStartViewActivity.java ob/b.java of/j.java w6/f.java
00036	Get resource file from res/raw directory	reflection	aa/e.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java of/j.java rc/e.java w6/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a5/b.java a5/c.java b1/f.java b1/g.java b1/m.java com/bugsnag/android/RootDetector.java com/bugsnag/android/a3.java com/bugsnag/android/r1.java com/bugsnag/android/u1.java e2/c.java e2/h.java g/r.java g/s.java i5/e.java l5/r.java ni/h.java sh/x.java w1/a.java x9/c.java
00091	Retrieve data from broadcast	collection	aa/l.java aa/q.java com/athenahealth/telehealth/ui/service/WaitingRoomService.java com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/priviamedicalgroup/priviaapp/ui/videoCall/presentation/view/VideoCallActivity.java rc/c.java
00162	Create InetSocketAddress object and connecting to it	socket	ai/c.java ai/k.java
00163	Create new Socket and connecting to it	socket	ai/c.java ai/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	c4/f.java c4/j.java t/u0.java
00089	Connect to a URL and receive input stream from the server	command network	c4/f.java c4/j.java com/bugsnag/android/g0.java com/bumptech/glide/load/data/j.java p7/a3.java p7/o5.java t/u0.java y9/c.java
00109	Connect to a URL and get the response code	network command	c4/f.java c4/j.java com/bumptech/glide/load/data/j.java p7/a3.java p7/o5.java q6/b.java t/u0.java y9/c.java
00189	Get the content of a SMS message	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java g1/e.java
00188	Get the address of a SMS message	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java g1/e.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java hf/x.java
00200	Query data from the contact list	collection contact	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java g1/e.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java g1/e.java
00201	Query data from the call log	collection calllog	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java g1/e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d5/a.java g1/e.java
00102	Set the phone speaker on	command	com/vidyo/lmi/audio/AudioCentral.java u3/b.java x3/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/bugsnag/android/NativeInterface.java com/bugsnag/android/m1.java com/bugsnag/android/ndk/NativeBridge.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/insurance/AddInsuranceFragment.java com/priviamedicalgroup/priviaapp/ui/messaging/presentation/view/SendMessagesFragment.java l2/d.java m2/a.java
00012	Read data and put it into a buffer stream	file	w1/a.java
00192	Get messages in the SMS inbox	sms	com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/insurance/AddInsuranceFragment.java
00125	Check if the given file path exist	file	com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/insurance/PreviewFragment.java of/j.java
00094	Connect to a URL and read data from it	command network	p7/a3.java p7/o5.java
00108	Read the input stream from given URL	network command	p7/a3.java p7/o5.java
00079	Hide the current app's icon	evasion	f3/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00114	Create a secure socket connection to the proxy address	network command	wh/i.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java p7/a3.java
00014	Read file into a stream and put it into a JSON object	file	x9/c.java
00147	Get the time of current location	collection location	g/g.java
00075	Get location of the device	collection location	g/g.java
00137	Get last known location of the device	location collection	g/g.java
00115	Get last known location of the device	collection location	g/g.java
00183	Get current camera parameters and change the setting.	camera	org/amazon/chime/webrtc/Camera1Session.java
00056	Modify voice volume	control	org/amazon/chime/webrtc/audio/WebRtcAudioTrack.java org/amazon/chime/webrtc/voiceengine/WebRtcAudioTrack.java
00121	Create a directory	file command	com/priviamedicalgroup/priviaapp/ui/manageAccount/presentation/view/fragment/BrowserFragment.java of/j.java
00112	Get the date of the calendar event	collection calendar	com/bugsnag/android/r2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00208	Capture the contents of the device screen	collection screen	org/amazon/chime/webrtc/ScreenCapturerAndroid.java
00199	Stop recording and release recording resources	record	org/amazon/chime/webrtc/CameraCapturer.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://mypriviaapp.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/598254641602/namespaces/firebase:fetch?key=AIzaSyB-8HMA1tWC4gQvFRHHktFk9ffE1F9UUhU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.priviahealth.com	ok	**IP:** 162.159.134.42 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bugsnag-notifications.privia.io	ok	**IP:** 34.149.142.15 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
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
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
px-shell-api-prod-v2021-08-13.px.athena.io	ok	**IP:** 52.0.100.122 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
bugsnag.com	ok	**IP:** 18.238.96.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mypriviaapp.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
secure.priviahealth.com	ok	**IP:** 34.54.0.57 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
bugsnag-session.privia.io	ok	**IP:** 34.149.142.15 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.onesignal.com	ok	**IP:** 104.16.160.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
docs.bugsnag.com	ok	**IP:** 18.155.173.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.myprivia.com	ok	**IP:** 23.220.73.40 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
px-shell-api-prview-v2021-08-13.px.athena.io	ok	**IP:** 35.169.197.122 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gl	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	w6/s.java
medicalrecords@priviahealth.com help@priviahealth.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://mypriviaapp.firebaseio.com"
"google_api_key" : "AIzaSyB-8HMA1tWC4gQvFRHHktFk9ffE1F9UUhU"
"google_crash_reporting_api_key" : "AIzaSyB-8HMA1tWC4gQvFRHHktFk9ffE1F9UUhU"
"your_session_expired_title" : "Alert"
5181942b9ebc31ce68dacb56c16fd79f
c682b8144a8dd52bc1ad63
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
2ed2c7bd-0fd2-41f9-bab8-93907be93e10

PLAYSTORE INFORMATION

Title: myPrivia

Score: 4.035714 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.priviamedicalgroup.priviaapp

Developer Details: Privia Health LLC, Privia+Health+LLC, None, http://www.priviahealth.com, help@priviahealth.com,

Release Date: Apr 10, 2018 **Privacy Policy:** Privacy link

Description:

myPrivia makes it easy for you to stay connected to your healthcare. Our secure log-in enables a more personalized experience, including easy access to your care team and tailored health content. The new layout features an at-a-glance view of alerts and upcoming appointments, the ability to check-in or start a virtual visit with one tap, and manage your prescriptions. myPrivia offers convenience and personalized care, delivering your health your way.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 07:54:49	Generating Hashes	OK

2025-09-01 07:54:49	Extracting APK	OK
2025-09-01 07:54:49	Unzipping	OK
2025-09-01 07:54:49	Parsing APK with androguard	OK
2025-09-01 07:54:49	Extracting APK features using aapt/aapt2	OK
2025-09-01 07:54:50	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 07:54:52	Parsing AndroidManifest.xml	OK
2025-09-01 07:54:52	Extracting Manifest Data	OK
2025-09-01 07:54:52	Manifest Analysis Started	OK
2025-09-01 07:54:53	Reading Network Security config from network_security_config.xml	OK
2025-09-01 07:54:53	Parsing Network Security config	OK
2025-09-01 07:54:53	Performing Static Analysis on: myPrivia (com.priviamedicalgroup.priviaapp)	OK

2025-09-01 07:54:54	Fetching Details from Play Store: com.priviamedicalgroup.priviaapp	OK
2025-09-01 07:54:56	Checking for Malware Permissions	OK
2025-09-01 07:54:56	Fetching icon path	OK
2025-09-01 07:54:56	Library Binary Analysis Started	OK
2025-09-01 07:54:56	Reading Code Signing Certificate	OK
2025-09-01 07:54:57	Running APKiD 2.1.5	OK
2025-09-01 07:54:59	Detecting Trackers	OK
2025-09-01 07:55:01	Decompiling APK to Java with JADX	OK
2025-09-01 07:55:31	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 07:55:31	Decompiling classes.dex with JADX	OK

2025-09-01 07:55:40	Decompiling with JADX failed for classes.dex	OK
2025-09-01 07:55:40	Decompiling classes.dex with JADX	OK
2025-09-01 07:56:04	Decompiling with JADX failed for classes.dex	OK
2025-09-01 07:56:04	Some DEX files failed to decompile	OK
2025-09-01 07:56:04	Converting DEX to Smali	OK
2025-09-01 07:56:04	Code Analysis Started on - java_source	OK
2025-09-01 07:56:06	Android SBOM Analysis Completed	OK
2025-09-01 07:56:13	Android SAST Completed	OK
2025-09-01 07:56:13	Android API Analysis Started	OK
2025-09-01 07:56:20	Android API Analysis Completed	OK
2025-09-01 07:56:21	Android Permission Mapping Started	OK

2025-09-01 07:56:29	Android Permission Mapping Completed	OK
2025-09-01 07:56:30	Android Behaviour Analysis Started	OK
2025-09-01 07:56:38	Android Behaviour Analysis Completed	OK
2025-09-01 07:56:38	Extracting Emails and URLs from Source Code	OK
2025-09-01 07:56:40	Email and URL Extraction Completed	OK
2025-09-01 07:56:40	Extracting String data from APK	OK
2025-09-01 07:56:40	Extracting String data from Code	OK
2025-09-01 07:56:40	Extracting String values and entropies from Code	OK
2025-09-01 07:56:43	Performing Malware check on extracted domains	OK
2025-09-01 07:56:45	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.