MOBSF

ANDROID STATIC ANALYSIS REPORT

MyUPMC (3.21.0)

File Name:	com.upmc.enterprises.myupmc_134.apk
Package Name:	com.upmc.enterprises.myupmc
Scan Date:	Sept. 1, 2025, 11 a.m.
App Security Score:	43/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	14	1	1	1

FILE INFORMATION

File Name: com.upmc.enterprises.myupmc_134.apk
Size: 41.02MB
MD5: 4818b76014c2d3bbadd6559ad4fab4a8
SHA1: fb9af94f5176ff9697b4933351107c117a3ebae5
SHA256: ae7262856660c66630153fee0af3077a52e843acc3d6a18679e14e10a3724d62

APP INFORMATION

App Name: MyUPMC
Package Name: com.upmc.enterprises.myupmc

Main Activity: com.upmc.enterprises.myupmc.LaunchActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 3.21.0
Android Version Code: 134

APP COMPONENTS

Activities: 10
Services: 11
Receivers: 4
Providers: 4
Exported Activities: 2
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
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: 2018-06-25 17:08:57+00:00
Valid To: 2048-06-25 17:08:57+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4412dcc56c3227c33a5ab96ab68405a980b1042d
Hash Algorithm: sha256
md5: 2df1f3b194b7bee328a2d5bf361cf0e2
sha1: 20cf96849100f381fcaf328068bb6ce86edd1f77
sha256: 5bc078a9606bb54416306f4e17e2565f6ad3dcb7a7f71d38a639df2918462598
sha512: e81027551388e5f104d43dbe1c9d2700c1c8548519616e2d51c161938c5426af4ca88928bd4e0b39270a7980e08f3a1d67245aa9c7987552f6bdb60c9ca89a74
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 4361399057dd5f6fad8fdb046c0398c99aa356fa3cdf9fc0d78aa92698fb322c
Found 1 unique certificates

APPLICATION PERMISSIONS

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.upmc.enterprises.myupmc.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>4818b76014c2d3bbadd6559ad4fab4a8.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></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.MANUFACTURER 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>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.upmc.enterprises.myupmc.LaunchActivity	Schemes: com.upmc.enterprises.myupmc://, https://, Hosts: myupmc.upmc.com, myupmc.page.link, Paths: /account-settings, /health-summary/documents-center/documents/additional-documents, /health-summary/medical-record/allergies, /appointments, /billing-and-insurance/billing, /health-summary/medical-record/covid-records, /account-settings/deactivate-account, /health-summary/documents-center/documents, /echeckin, /appointments/find-care/other-care-options/edermatology, /account-settings/notification-preferences/email-notifications, /billing-and-insurance/estimates, /account-settings/family-access, /fastpass, /support/faqs, /appointments/find-care/find-a-new-provider, /appointments/find-care, /appointments/find-care/care-team, /health-summary/medical-record/current-health-issues, /billing-and-insurance/health-plan, /support/help-and-feedback, /health-summary/medical-record/immunizations, /health-summary/documents-center/letters, /login, /health-summary/medical-record, /health-summary/medical-record/medications, /messages, /account-settings/notification-preferences, /appointments/find-care/other-care-options, /account-settings/patient-information, /health-summary/medical-record/questionnaires, /appointments/scheduling/care-team, /terms-and-conditions, /health-summary/medical-record/test-results, /account-settings/notification-preferences/text-notifications, /xealth,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.upmc.enterprises.myupmc://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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.upmc.enterprises.myupmc.guest.GuestActivity) 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.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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
6	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/upmc/enterprises/myupmc/BuildConfig.java com/upmc/enterprises/myupmc/customizablealert/CustomizableAlertService.java com/upmc/enterprises/myupmc/findcare/findaprovider/domain/usecase/GenerateFindAProviderLinkUseCase.java com/upmc/enterprises/myupmc/findcare/findaprovider/ui/FindAProviderConstants.java com/upmc/enterprises/myupmc/guestscreen/GuestTestimonialModel.java com/upmc/enterprises/myupmc/guestscreen/page/GuestScreenTestimonialPageFragment.java com/upmc/enterprises/myupmc/login/LoginFragmentDirections.java com/upmc/enterprises/myupmc/more/settings/changepassword/network/ChangePasswordAuthenticatedBody.java com/upmc/enterprises/myupmc/more/settings/changepassword/network/ChangePasswordUnauthenticatedBody.java com/upmc/enterprises/myupmc/onboarding/page/OnBoardingPageFragment.java com/upmc/enterprises/myupmc/patient/data/mapper/PushNotificationTypeMapper.java com/upmc/enterprises/myupmc/services/OnboardingInteractionService.java com/upmc/enterprises/myupmc/services/RatingsPromptService.java com/upmc/enterprises/myupmc/services/SessionCountService.java com/upmc/enterprises/myupmc/services/UpdateContactInfoService.java com/upmc/enterprises/myupmc/services/firebase/FirebaseAnalyticsConstants.java com/upmc/enterprises/myupmc/shared/analytics/AnalyticsThirdPartyConstants.java com/upmc/enterprises/myupmc/shared/auth/domain/model/SessionTokensDomainModel.java com/upmc/enterprises/myupmc/shared/healthbeat/healthbeatcard/page/HealthBeatCardPageFragment.java com/upmc/enterprises/myupmc/shared/navigation/dialog/GenericAlertDialogConfig.java com/upmc/enterprises/myupmc/shared/navigation/navigators/ActivityWithResultNavigator.java com/upmc/enterprises/myupmc/shared/navigation/navigators/ChromeCustomTabsNavigator.java com/upmc/enterprises/myupmc/shared/push/PushTokensConfig.java com/upmc/enterprises/myupmc/shared/services/auth/model/TokenResponse.java com/upmc/enterprises/myupmc/shared/services/auth/model/UserMetadataResponse.java com/upmc/enterprises/myupmc/shared/services/firebase/FirebaseAnalyticsConstants.java com/upmc/enterprises/myupmc/shared/services/firebase/FirebaseMessagingManager.java com/upmc/enterprises/myupmc/shared/services/push/MyUpmcPushNotificationService.java com/upmc/enterprises/myupmc/shared/termsandconditions/TermsAndConditionsConfig.java com/upmc/enterprises/myupmc/user/UserMetadataModel.java com/upmc/enterprises/myupmc/whatsnew/WhatsNewService.java com/upmc/enterprises/myupmc/workflow/WorkflowConstants.java io/reactivex/rxjava3/internal/schedulers/SchedulerPoolFactory.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/contentful/rich/android/renderer/views/HyperLinkRenderer.java com/oliverspryn/library/MainKt.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java timber/log/Timber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/airbnb/lottie/network/NetworkCache.java pro/piwik/sdk/tools/Checksum.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/contentful/java/cda/CDAClient.java com/upmc/enterprises/myupmc/appointments/dagger/modules/AppointmentApiServiceModule.java com/upmc/enterprises/myupmc/dagger/modules/DeactivateAccountModule.java com/upmc/enterprises/myupmc/dagger/modules/PatientNotificationsModule.java com/upmc/enterprises/myupmc/dagger/modules/PushNotificationModule.java com/upmc/enterprises/myupmc/dagger/modules/SystemStatusModule.java com/upmc/enterprises/myupmc/dagger/modules/UserServiceModule.java com/upmc/enterprises/myupmc/dagger/modules/XealthModule.java com/upmc/enterprises/myupmc/insurance/dagger/modules/InsuranceServiceModule.java com/upmc/enterprises/myupmc/shared/dagger/modules/AuthModule.java com/upmc/enterprises/myupmc/shared/dagger/modules/HealthBeatModule.java com/upmc/enterprises/myupmc/shared/dagger/modules/TermsAndConditionsModule.java com/upmc/enterprises/myupmc/shared/dagger/modules/UserDeviceModule.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	coil/decode/SourceImageSource.java
6	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	com/upmc/enterprises/myupmc/shared/services/crypto/CryptographyManager.java
7	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/upmc/enterprises/myupmc/shared/navigation/browser/ui/MyUpmcBrowserController.java
8	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	pro/piwik/sdk/Tracker.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/upmc/enterprises/myupmc/shared/dagger/modules/AndroidModule.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	com/contentful/rich/android/renderer/views/HyperLinkRenderer.java com/upmc/enterprises/myupmc/dashboard/DashboardController.java com/upmc/enterprises/myupmc/shared/navigation/browser/domain/usecase/DownloadFileUseCase.java com/upmc/enterprises/myupmc/shared/navigation/browser/domain/usecase/InterceptUrlRequestUseCase.java com/upmc/enterprises/myupmc/shared/navigation/navigators/HttpNavigator.java
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java okio/Okio__JvmOkioKt.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java pro/piwik/sdk/dispatcher/EventDiskCache.java pro/piwik/sdk/tools/Checksum.java
00091	Retrieve data from broadcast	collection	com/upmc/enterprises/myupmc/MainController.java com/upmc/enterprises/myupmc/dashboard/DashboardController.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/upmc/enterprises/myupmc/dashboard/DashboardController.java com/upmc/enterprises/myupmc/shared/navigation/browser/domain/usecase/InterceptUrlRequestUseCase.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java
00023	Start another application from current application	reflection control	com/upmc/enterprises/myupmc/shared/navigation/navigators/ExternalAppNavigator.java
00162	Create InetSocketAddress object and connecting to it	socket	com/upmc/enterprises/myupmc/shared/services/NetworkConnectivityService.java
00163	Create new Socket and connecting to it	socket	com/upmc/enterprises/myupmc/shared/services/NetworkConnectivityService.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/contentful/rich/android/renderer/views/HyperLinkRenderer.java com/upmc/enterprises/myupmc/shared/navigation/browser/domain/usecase/DownloadFileUseCase.java
00089	Connect to a URL and receive input stream from the server	command network	pro/piwik/sdk/dispatcher/Dispatcher.java
00109	Connect to a URL and get the response code	network command	pro/piwik/sdk/dispatcher/Dispatcher.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/LottieCompositionFactory.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00191	Get messages in the SMS inbox	sms	com/upmc/enterprises/myupmc/shared/navigation/browser/domain/usecase/DownloadFileUseCase.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Open Firebase database	high	The Firebase database at https://n320xns0lwpch8t.firebaseio.com/.json is exposed to internet without any authentication
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/280525754468/namespaces/firebase:fetch?key=AIzaSyA6SggQy2uYaHWQazotdGmNfaD6YlzJT3k is enabled. Ensure that the configurations are not sensiti quesid=9999999997&a', 'covid_vaccine_button_url_use_auth_context': 'true', 'covid_vaccine_button_url_use_auth_context_tst': 'true', 'covid_vaccine_header': 'Covid-19 Vaccine Sign-up', 'covid_vaccine_header_tst': 'Covid-19 Vaccine Sign-up', 'covi device\'s "Do Not Disturb" settings and update your preferences. For help, please visit our MyUPMC FAQs.', 'customizable_alert_title': '', 'customizable_alert_title_tst': 'Custom Alert', 'deactivate_account_is_enabled': 'true', 'deactivate_account_is_ vaccine from UPMC now.', 'flu_shot_button_text': 'Register Now', 'flu_shot_button_text_tst': 'Register Now', 'flu_shot_button_url': 'https://vaccine.upmc.com/?utm_source=myupmc&utm_medium=internal&utm_content=covid-vaccine&utm_camp '1010101,1010117,1010141,1010146,1010162,1010163,1010166,1010170,1010171,1010172,1010179,10616001,10641001,10641002,1011487001,1011487002,1011781001,100020014042,10358011,10373002,10373003,10373004,10373005,1037 'questionnaire_department_ids_tst': '1010101,1010117,1010141,1010146,1010162,1010163,1010166,1010170,1010171,1010172,1010179,10616001,10641001,10641002,1011487001,1011487002,1011781001,100020014042,10358011,10373002,10373003,10373004,10373005,1037 'renew_prescription_whats_new_flag_v1': 'false', 'renew_prescription_whats_new_flag_v9_tst': 'true', 'request_appointment_is_enabled': 'false', 'request_appointment_is_enabled_tst': 'true', 'schedule_appt_whats_new_flag_v1': 'false', 'schedule_a 'web_analytics_is_enabled_tst': 'false', 'whats_new_body_text': 'Use our new COVID-19 Screening Tool to understand your risk and next steps for care.', 'whats_new_body_text_tst': 'Update test As a reminder, most lab and imaging test results ar

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
upmc.mysecurebill.com	ok	**IP:** 67.196.187.165 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **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
bing.com	ok	**IP:** 150.171.27.10 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.upmc.com	ok	**IP:** 151.195.136.79 **Country:** United States of America **Region:** Pennsylvania **City:** Pittsburgh **Latitude:** 40.444321 **Longitude:** -79.954918 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.bing.com	ok	**IP:** 23.62.226.36 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
cdn.contentful.com	ok	**IP:** 151.101.199.18 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.healthwise.net	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.google.com	ok	**IP:** 142.250.72.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ccp.mysecurebill.com	ok	**IP:** 67.196.187.165 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
myupmc.upmc.com	ok	**IP:** 54.83.33.203 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
upmc.piwik.pro	ok	**IP:** 20.246.225.201 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
api.myupmc.upmce.net	ok	**IP:** 34.238.203.109 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.youtube.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
providers.upmc.com	ok	**IP:** 45.60.233.26 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
status.myupmc.upmce.net	ok	**IP:** 18.238.109.45 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
upmc.com	ok	**IP:** 151.195.136.79 **Country:** United States of America **Region:** Pennsylvania **City:** Pittsburgh **Latitude:** 40.444321 **Longitude:** -79.954918 **View:** Google Map
n320xns0lwpch8t.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
images.ctfassets.net	ok	**IP:** 18.155.173.10 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
tst.myupmc.upmce.net	ok	**IP:** 54.197.74.29 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
preview.contentful.com	ok	**IP:** 151.101.199.18 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
share.upmc.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://n320xns0lwpch8t.firebaseio.com"
"google_api_key" : "AIzaSyA6SggQy2uYaHWQazotdGmNfaD6YlzJT3k"
"google_crash_reporting_api_key" : "AIzaSyA6SggQy2uYaHWQazotdGmNfaD6YlzJT3k"
"login_password" : "Password"
"login_username" : "Username"
8ccb2ecab23b755b7c2cce5aa7a6b414
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
64ebd52e-d004-469a-a6e7-2263940dbf41
1D16FEE2-A934-4868-9CF9-DAB1625FA6E1
23456789abcdefghjkmnpqrstvwxyz

POSSIBLE SECRETS
4C3C65CF-D22E-48D8-B60B-182485D6108C
8F938D02-27FA-4DEA-9B1F-7C35FFE5CDEA
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
5771F100-509A-4A0C-AA42-95C4981692F7
ACC8F240-7038-451F-9AFE-F4E8FA7177D3
nMui2HO8zTbwFxONUrmYXIOTKL3g
0F4915BF-E1B3-452C-ACB5-6068BD2B0051

PLAYSTORE INFORMATION

Title: MyUPMC

Score: 4.410385 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.upmc.enterprises.myupmc

Developer Details: UPMC, UPMC, None, https://myupmc.upmc.com, MyUPMC_Feedback@upmc.edu,

Release Date: Jul 21, 2018 **Privacy Policy:** Privacy link

Description:

Manage your health information anywhere, anytime, with MyUPMC. With the MyUPMC app, you can easily communicate with your UPMC doctors, access family medical records, and manage your appointments, all from your mobile device. With MyUPMC, you can: • Send a message directly to your doctor’s office anytime • Schedule appointments with UPMC providers • Access your medical records and doctors' notes • Conveniently manage your family's health • See your test results, medications, immunization history, and more • Manage your appointments and save to your calendar • Renew prescriptions without calling your doctor’s office • Quickly view and pay your bills • Find a UPMC doctor, including primary, pediatric, and specialty care providers, and request to schedule an appointment. Access is convenient, free, and secure! For the best experience, please update your mobile device and tablet to the latest operating system. If you experience issues, completely close the app, restart your device and open the application. Encounter a problem? Need to ask a question? Please call the MyUPMC Support line at 1-866-884-8579, option 2. Have a suggestion or feedback? Email MyUPMC_Feedback@upmc.edu. Thank you! Enjoying the MyUPMC app? Rate it now and let us know.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 11:00:42	Generating Hashes	OK
2025-09-01 11:00:43	Extracting APK	OK
2025-09-01 11:00:43	Unzipping	OK
2025-09-01 11:00:44	Parsing APK with androguard	OK

2025-09-01 11:00:44	Extracting APK features using aapt/aapt2	OK
2025-09-01 11:00:44	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 11:00:46	Parsing AndroidManifest.xml	OK
2025-09-01 11:00:47	Extracting Manifest Data	OK
2025-09-01 11:00:47	Manifest Analysis Started	OK
2025-09-01 11:00:50	Reading Network Security config from network_security_config.xml	OK
2025-09-01 11:00:50	Parsing Network Security config	OK
2025-09-01 11:00:50	Performing Static Analysis on: MyUPMC (com.upmc.enterprises.myupmc)	OK
2025-09-01 11:00:52	Fetching Details from Play Store: com.upmc.enterprises.myupmc	OK
2025-09-01 11:00:54	Checking for Malware Permissions	OK
2025-09-01 11:00:54	Fetching icon path	OK
2025-09-01 11:00:54	Library Binary Analysis Started	OK
2025-09-01 11:00:56	Reading Code Signing Certificate	OK
2025-09-01 11:00:56	Running APKiD 2.1.5	OK
2025-09-01 11:01:05	Detecting Trackers	OK
2025-09-01 11:01:18	Decompiling APK to Java with JADX	OK
2025-09-01 11:01:37	Decompiling with JADX failed, attempting on all DEX files	OK

2025-09-01 11:01:37	Decompiling classes2.dex with JADX	OK
2025-09-01 11:01:47	Decompiling classes4.dex with JADX	OK
2025-09-01 11:01:57	Decompiling classes.dex with JADX	OK
2025-09-01 11:02:35	Decompiling classes3.dex with JADX	OK
2025-09-01 11:02:44	Decompiling classes5.dex with JADX	OK
2025-09-01 11:02:47	Decompiling classes2.dex with JADX	OK
2025-09-01 11:02:55	Decompiling classes4.dex with JADX	OK
2025-09-01 11:03:03	Decompiling classes.dex with JADX	OK
2025-09-01 11:03:13	Decompiling classes3.dex with JADX	OK
2025-09-01 11:03:21	Decompiling classes5.dex with JADX	OK
2025-09-01 11:03:24	Converting DEX to Smali	OK
2025-09-01 11:03:24	Code Analysis Started on - java_source	OK
2025-09-01 11:03:28	Android SBOM Analysis Completed	OK
2025-09-01 11:03:36	Android SAST Completed	OK
2025-09-01 11:03:36	Android API Analysis Started	OK
2025-09-01 11:03:41	Android API Analysis Completed	OK
2025-09-01 11:03:42	Android Permission Mapping Started	OK

2025-09-01 11:03:46	Android Permission Mapping Completed	OK
2025-09-01 11:03:47	Android Behaviour Analysis Started	OK
2025-09-01 11:03:54	Android Behaviour Analysis Completed	OK
2025-09-01 11:03:54	Extracting Emails and URLs from Source Code	OK
2025-09-01 11:03:57	Email and URL Extraction Completed	OK
2025-09-01 11:03:57	Extracting String data from APK	OK
2025-09-01 11:03:57	Extracting String data from Code	OK
2025-09-01 11:03:57	Extracting String values and entropies from Code	OK
2025-09-01 11:04:04	Performing Malware check on extracted domains	OK
2025-09-01 11:04:09	Saving to Database	OK
