ANDROID STATIC ANALYSIS REPORT

athenaPatient (1.21.0)

File Name:	com.athenahealth.athenapatient_71.apk
Package Name:	com.athenahealth.athenapatient
Scan Date:	Aug. 29, 2025, 7:57 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	23	1	2	1

FILE INFORMATION

File Name: com.athenahealth.athenapatient_71.apk
Size: 10.76MB
MD5: 86097f71d22f84a21c1198259caaee17
SHA1: 48b3ca4218debf5ce5a6d3adcbb361c1f3395901
SHA256: 62fd3b238d80a5a2b29d8dd42068e18f67ad654037832b768e3e880ae685bc86

APP INFORMATION

App Name: athenaPatient
Package Name: com.athenahealth.athenapatient
Main Activity: com.athenahealth.athenapatient.MainActivity
Target SDK: 34
Min SDK: 30
Max SDK:
Android Version Name: 1.21.0

Android Version Code: 71

APP COMPONENTS

Activities: 12
Services: 13
Receivers: 15
Providers: 4
Exported Activities: 5
Exported Services: 1
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-10-18 02:48:18+00:00
Valid To: 2052-10-18 02:48:18+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xcb5d7d6388bcd5d49e9ea592a47552f6459c9178
Hash Algorithm: sha256
md5: 857c13602b08a0cf8f5d7a58ffa1ca9f
sha1: 0acaae1762654c35faccf4d6439ec9a9f911af2b
sha256: cb3b785f577e619787d324e5f08c703331311675c923fe96e601b6b1f0435bad
sha512: 9f7e33f33b47b1f00fc911e4789424e64fc545d9e65d2434b4ef843ef7d9b356eb2d1557820080b0838523ee220ec2dbde9a37a1c583abb63414c57ab681f346
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 64ec8d6b0bf3789f1e392be479501436e26c8aadaaf763fb044541733fa2ee2b
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.athenahealth.athenapatient.permission.C2D_MESSAGE	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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.athenahealth.athenapatient.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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.TAGS check
SIM operator check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.athenahealth.athenapatient.MainActivity	Schemes: app://, Hosts: com.athenahealth.portal, Path Prefixes: /selfScheduling,

ACTIVITY	INTENT
com.okta.webauthenticationui.RedirectActivity	Schemes: com.athenahealth.portal://,
com.okta.oidc.OktaRedirectActivity	Schemes: com.athenahealth.portal.legacy://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

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: **0** | WARNING: **14** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (com.okta.webauthenticationui.RedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Broadcast Receiver (com.onesignal.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.
4	Activity (com.onesignal.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.
5	Broadcast Receiver (com.onesignal.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.
6	Broadcast Receiver (com.onesignal.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.
7	Broadcast Receiver (com.onesignal.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
8	Activity (com.onesignal.NotificationOpenedReceiver) 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	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) 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.
10	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.
11	Activity (com.okta.oidc.OktaRedirectActivity) 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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	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.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	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: **1** | WARNING: **7** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a3/b.java ae/a.java b2/b.java b3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c0/e0.java c0/j.java c0/x.java cg/c.java com/athenahealth/athenapatient/a.java com/launchdarkly/sdk/android/g0.java com/okta/oidc/OIDCConfig.java com/okta/oidc/clients/web/SyncWebAuthClientImpl.java com/okta/oidc/net/request/TokenRequest.java com/okta/oidc/storage/security/EncryptionManagerAPI18.java com/okta/oidc/storage/security/EncryptionManagerAPI23.java com/okta/oidc/util/CodeVerifierUtil.java com/okta/oidc/util/UriUtil.java com/onesignal/JobIntentService.java com/onesignal/a4.java com/onesignal/e.java di/b.java e0/g.java e0/h.java e0/k.java e2/i.java fg/c.java fg/c0.java fg/d0.java fg/h0.java fg/i0.java fg/j.java fg/m0.java fg/q.java fg/s.java fg/u.java fg/v.java gd/b.java gd/c.java gd/e.java gd/l.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	gd/o.java gd/r.java gd/t.java gd/u.java gd/x.java hd/e.java hd/o.java jd/c0.java jd/c1.java jd/e.java jd/r0.java jd/s1.java jd/y.java jf/j.java kd/b.java kd/g0.java kd/k0.java kd/s.java kd/u.java kd/w0.java kd/y.java kf/h.java kf/k.java lb/f.java m1/i.java m1/j.java m1/r.java mc/b.java mc/c.java mc/g.java mc/h.java mc/i.java nk/b.java o0/a.java o0/e0.java o0/q.java r6/f.java s0/k.java s1/d.java sb/c.java sc/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sh/a.java uc/j.java v0/c.java ve/e.java vk/h.java w/f.java wk/d.java x3/c.java x3/g.java y/b.java z1/d.java zd/a.java zf/c.java
2	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/athenahealth/athenapatient/util/manager/FileSelectionManager.java oa/a.java ya/a.java
3	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	bg/c.java com/athenahealth/athenapatient/util/manager/FileSelectionManager.java oa/a.java
4	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/n0.java da/c.java da/g.java e0/h.java h3/h.java lh/h.java mj/a.java mj/b.java mk/y.java nj/a.java zk/d.java zk/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	ad/j.java ad/l.java ad/o.java com/onesignal/m4.java s1/c.java v4/d.java wh/a.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ng/h.java vk/c.java vk/d.java vk/g.java vk/h.java
7	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	bg/b.java cg/c.java fg/q.java na/d.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	jf/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/launchdarkly/sdk/LDContext.java com/okta/authfoundation/credential/SharedPreferencesTokenStorage.java com/okta/authfoundationbootstrap/CredentialBootstrap.java com/okta/legacytokenmigration/LegacyTokenMigration.java com/okta/oidc/net/request/ProviderConfiguration.java com/okta/oidc/net/request/web/WebRequest.java com/okta/oidc/net/response/TokenResponse.java com/okta/oidc/net/response/web/WebResponse.java k9/k.java k9/v.java
10	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/onesignal/z5.java
11	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/z5.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bg/c.java com/microsoft/appcenter/crashes/a.java ec/d.java f0/h.java gj/f.java h3/h.java j3/a.java j8/j.java j8/k.java k1/c.java k1/f.java l8/g.java o1/a.java uk/a.java xb/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/athenahealth/athenapatient/MainActivity.java com/okta/oidc/OktaAuthenticationActivity.java com/okta/oidc/util/AuthorizationException.java com/okta/webauthenticationui/DefaultWebAuthenticationProvider.java com/onesignal/OSUtils.java com/onesignal/i0.java com/onesignal/k4.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java fg/c.java h1/b.java hd/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/athenahealth/athenapatient/MainActivity.java com/okta/oidc/OktaAuthenticationActivity.java com/okta/webauthenticationui/DefaultWebAuthenticationProvider.java com/onesignal/OSUtils.java com/onesignal/i0.java com/onesignal/k4.java fg/c.java h1/b.java hd/e.java
00078	Get the network operator name	collection telephony	a3/a.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/onesignal/a4.java
00115	Get last known location of the device	collection location	a3/a.java g/e.java
00132	Query The ISO country code	telephony collection	a3/a.java com/microsoft/appcenter/utils/DeviceInfoHelper.java
00036	Get resource file from res/raw directory	reflection	com/onesignal/OSUtils.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java fg/c.java h1/b.java hd/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/launchdarkly/sdk/android/d0.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/a.java i8/g.java j3/a.java k3/c.java kh/b.java oa/g.java s1/d.java t1/a.java w2/b.java wh/c.java y2/f.java ya/a.java z8/a.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/Crashes.java w2/b.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/Crashes.java
00091	Retrieve data from broadcast	collection	com/okta/oidc/OktaAuthenticationActivity.java com/onesignal/FCMBroadcastReceiver.java com/onesignal/PermissionsActivity.java fg/k.java fg/u.java t9/c.java
00162	Create InetSocketAddress object and connecting to it	socket	vk/b.java vk/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	vk/b.java vk/h.java
00096	Connect to a URL and set request method	command network	com/okta/oidc/net/HttpClientImpl.java com/onesignal/s4.java h3/o.java sc/b.java
00089	Connect to a URL and receive input stream from the server	command network	cg/c.java com/okta/oidc/net/HttpClientImpl.java com/onesignal/s4.java sc/b.java
00109	Connect to a URL and get the response code	network command	cg/c.java com/okta/oidc/net/HttpClientImpl.java com/onesignal/s4.java sc/b.java
00012	Read data and put it into a buffer stream	file	l8/g.java
00009	Put data in cursor to JSON object	file	com/onesignal/n0.java com/onesignal/r0.java com/onesignal/t.java com/onesignal/u0.java w2/b.java
00094	Connect to a URL and read data from it	command network	fg/c.java lh/c.java
00014	Read file into a stream and put it into a JSON object	file	bg/c.java h3/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/athenahealth/athenapatient/util/manager/FileSelectionManager.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java h7/a.java l0/e.java
00188	Get the address of a SMS message	sms	com/athenahealth/athenapatient/util/manager/FileSelectionManager.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java h7/a.java l0/e.java
00200	Query data from the contact list	collection contact	com/athenahealth/athenapatient/util/manager/FileSelectionManager.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java h7/a.java l0/e.java
00201	Query data from the call log	collection calllog	com/athenahealth/athenapatient/util/manager/FileSelectionManager.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java h7/a.java l0/e.java
00092	Send broadcast	command	com/onesignal/r0.java
00147	Get the time of current location	collection location	g/e.java
00075	Get location of the device	collection location	g/e.java
00137	Get last known location of the device	location collection	g/e.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java l0/e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/athenahealth/athenapatient/util/manager/FileSelectionManager.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java l0/e.java
00023	Start another application from current application	reflection control	com/onesignal/a4.java
00125	Check if the given file path exist	file	com/onesignal/a4.java
00030	Connect to the remote server through the given URL	network	com/okta/oidc/net/HttpClientImpl.java
00153	Send binary data over HTTP	http	com/okta/oidc/net/HttpClientImpl.java
00114	Create a secure socket connection to the proxy address	network command	qk/f.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.CAMERA, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	3/44	android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE

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
firebase.google.com	ok	**IP:** 74.125.136.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
in.appcenter.ms	ok	**IP:** 68.220.193.245 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.818501 **Longitude:** -84.361015 **View:** Google Map
maps.googleapis.com	ok	**IP:** 108.177.122.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.docs.developers.amplitude.com	ok	**IP:** 76.76.21.123 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
mobile.launchdarkly.com	ok	**IP:** 23.20.148.186 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.athenahealth.com	ok	**IP:** 23.62.226.177 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
mobile.events.data.microsoft.com	ok	**IP:** 13.89.179.13 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map
clientsdk.launchdarkly.com	ok	**IP:** 151.101.193.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 18.185.210.151 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 64.233.185.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api2.amplitude.com	ok	**IP:** 44.240.171.47 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.17.111.223 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
athenahealthrc.iad1.qualtrics.com	ok	**IP:** 23.202.57.104 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.253.124.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pxppapp.px.athena.io	ok	**IP:** 18.155.173.8 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
clientstream.launchdarkly.com	ok	**IP:** 76.223.31.44 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	hd/n.java

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
7fc993f702adc9ebeb88966e865382cf8e04333b670d92e27f0bcd31cb651a1e
3b904b8655e84bf58c673c070a5512b9406a617b830ea055a6050761f2873908
caf9fbe573bed5a11b80a8115a0ef2f2c601764f118e1879d61b0248b20fd5d4
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
0c5dbeef-d2c0-4a10-9c12-b8f29905b426
cd57aa89bfab572ea38a59d647737a0eb7987f1cffad631dca6ef60f9e0d3d30
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
9fa9d447bd839b1fa8094ae3cdd0637f65a7d9652146b281c1be7f87724086a7
4055de0dc85b3bfc04488736f01e2e762abb1b48ad0c5374e7095f2d194a7b84
3ca0bcde7fc12d96c7168529eb9be8011be7f5fc9876126c5e5598757b2e3ecd
169cf5d7dcbb1d39c6e4ffdaf27e6623e96f084dbab0330a4f459e3790d864b5
9ecc0927f93ddd6000571be5550b9c350151f57ab65ea5497526c9c26fd16b34
046a56bbe89e4070eb0a0027f6dcc608a651a2f2d53618d3b11231644feb32c2
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
09ae9b1294eaf7af2b7f2bd8ec3dcd416ac9fb8986353e346e424b40252bc89a
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
a323ce3ad90a978ea2324ac88a7702060ea2474d2b85aa1107e937edfc2c8da0
bbefdee03c1ef93ea0f22eebd8fe33caefe3417fa84f4040dad0dd55b3b7dd98
29be66199e75450cc8d3ab075269b37ce9d459683513cecdf67e024d3ed389e7
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
061ef5a10484818bcacf3153a9713de60dff3f2502923813a3bf938a93256d28
20142ccb9046adf0bc795bf37e9e28defa6767ad4aa0612376d1883a2c1775b5
c682b8144a8dd52bc1ad63
5151174860936688c89b2bfd0fa3c9e8e8832d8dbd8062f5233897dc232331d0
245f131c-3112-4d9c-b4ec-991915ae0b3d
25b5cd64a15fff0a05958ecede0bd86dd229de41c70152a77128e2784a6d48f7
5eb5a37e-b458-11e3-ac11-000c2940e62c

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
99224ff3a21402f64b6bdddad36e6214681c5f30088d968de3d7028c453274af
27030a3ff4a47387ef5fbc9358ffad8678b3702f15e281f0f6c790f3e1099952
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
f5012515086ec4488241748623cec55736a0b04d7293a870ef7875a96badfe67
115792089210356248762697446949407573530086143415290314195533631308867097853951
b0ba75ba49bc3e204c82e2aa247717e64
b-9a7ebb56-5722-4903-a675-318e899925db
5181942b9ebc31ce68dacb56c16fd79f
67e7ac52868cbbea640a4e41594c4df562c21bab892341ae69a29a8047ac8daf
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449
b-13bbaada-86f8-497d-9ef6-563622d70239
ac7b3a3d55d5900cb3699e0b75afd2d4

POSSIBLE SECRETS
ee11eb45810b93a532f9b63a74697ae9bfc8c2f1d601f71fe2e70cf55388034e
dfb01d686a64e991725a07b9d7bbb7854b302e5f2aed2864df01e91b3526e2e7
efbff1001e3eb51ee52e4de9a7c21fb52ee7ba28387ea373bbf2214565e45c2f
e02ec956c454927b908ea5277c0f4f66a98865170a8a6384704f9627aee666cb
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
26720484c9a0738570500d9b11f1c64db03271f498c42dfbdac7cae61f9b4ef9
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: athenaPatient

Score: 4.817259 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.athenahealth.athenapatient

Developer Details: athenahealth, athenahealth, None, https://athenahealth.com, info@athenahealth.com,

Release Date: Nov 9, 2022 **Privacy Policy:** Privacy link

Description:

athenaPatient is only available for patients whose healthcare providers have instructed them to download and use the app. Access your health information and communicate with your care team anywhere, anytime.* athenaPatient is a convenient, mobile resource that allows you to: - Log in quickly – Facial recognition and touch ID make log in easy while keeping your data safe. - View test results – Access lab, imaging, and other medical test results as soon as they become available. - Message your care team – Contact your care team whenever you have questions through quick, secure direct messages. - Self-schedule appointments – Book appointments with your care team and view upcoming visits beyond regular office hours. Your provider(s) must support Self-Scheduling to use this feature. - Check in before your visit – Easily check in for appointments and save time by completing any necessary documentation before your arrival. (Your provider(s) must support Self Check-In to use this feature) - Attend virtual visits – Easily initiate and attend telehealth visits with members of your care team. (Your provider(s) must support virtual visits through athenaTelehealth to use this feature.) - Get directions to appointments – Driving directions show you how to get to your next medical appointment. Please note that you must have an existing athenahealth Patient Portal account to use athenaPatient. Once you've downloaded and launched athenaPatient, you must log in using the same email address and password you use to access your provider's athenahealth Patient Portal to begin using the app. It will ask if you want to enable Face ID or Touch ID. Enabling either of these features will save you from having to enter your login information every time you want to use the app. If you do not have your Patient Portal account information, your healthcare provider(s) may offer Patient Portal access through their website. If you're having issues finding your healthcare provider's Patient Portal, you can contact their office for the correct URL, or to request an email invitation to their Patient Portal. * The athenaPatient app is only available for download and viewing information in the United States for patients of healthcare providers on the athenahealth network.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:57:27	Generating Hashes	OK
2025-08-29 19:57:27	Extracting APK	OK
2025-08-29 19:57:27	Unzipping	OK
2025-08-29 19:57:27	Parsing APK with androguard	OK
2025-08-29 19:57:27	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:57:27	Getting Hardcoded Certificates/Keystores	OK

2025-08-29 19:57:29	Parsing AndroidManifest.xml	OK
2025-08-29 19:57:29	Extracting Manifest Data	OK
2025-08-29 19:57:29	Manifest Analysis Started	OK
2025-08-29 19:57:29	Reading Network Security config from network_security_config.xml	OK
2025-08-29 19:57:29	Parsing Network Security config	OK
2025-08-29 19:57:29	Performing Static Analysis on: athenaPatient (com.athenahealth.athenapatient)	OK
2025-08-29 19:57:30	Fetching Details from Play Store: com.athenahealth.athenapatient	OK
2025-08-29 19:57:31	Checking for Malware Permissions	OK
2025-08-29 19:57:31	Fetching icon path	OK
2025-08-29 19:57:31	Library Binary Analysis Started	OK

2025-08-29 19:57:31	Reading Code Signing Certificate	OK
2025-08-29 19:57:31	Running APKiD 2.1.5	OK
2025-08-29 19:57:32	Detecting Trackers	OK
2025-08-29 19:57:34	Decompiling APK to Java with JADX	OK
2025-08-29 19:57:44	Converting DEX to Smali	OK
2025-08-29 19:57:44	Code Analysis Started on - java_source	OK
2025-08-29 19:57:46	Android SBOM Analysis Completed	OK
2025-08-29 19:57:53	Android SAST Completed	OK
2025-08-29 19:57:53	Android API Analysis Started	OK
2025-08-29 19:58:00	Android API Analysis Completed	OK
2025-08-29 19:58:00	Android Permission Mapping Started	OK

2025-08-29 19:58:05	Android Permission Mapping Completed	OK
2025-08-29 19:58:05	Android Behaviour Analysis Started	OK
2025-08-29 19:58:12	Android Behaviour Analysis Completed	OK
2025-08-29 19:58:13	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:58:15	Email and URL Extraction Completed	OK
2025-08-29 19:58:15	Extracting String data from APK	OK
2025-08-29 19:58:15	Extracting String data from Code	OK
2025-08-29 19:58:15	Extracting String values and entropies from Code	OK
2025-08-29 19:58:16	Performing Malware check on extracted domains	OK
2025-08-29 19:58:20	Saving to Database	OK

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.