

ANDROID STATIC ANALYSIS REPORT



Aetna Better Health - Medicaid (7.4)

File Name:	com.aetna.aetnabetterhealthmobile_101.apk
Package Name:	com.aetna.aetnabetterhealthmobile
Scan Date:	Aug. 29, 2025, 7:06 p.m.
App Security Score:	58/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

兼HIGH	▲ MEDIUM	i INFO	✓ SECURE	@ HOTSPOT
2	15	2	4	2

FILE INFORMATION

File Name: com.aetna.aetnabetterhealthmobile_101.apk

Size: 28.26MB

MD5: 13e552e26a564386b048603efb18164e

SHA1: 6d23874a7764540210356574e1a61d344656292e

SHA256: 14214c77a5bf5ed3ce41ecd6870a65089475a1222e1d281a1ed034c0bd1f6995

i APP INFORMATION

App Name: Aetna Better Health - Medicaid

Package Name: com.aetna.aetnabetterhealthmobile

Main Activity: com.aetna.aetnabetterhealthmobile.SplashActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 7.4
Android Version Code: 101



Activities: 38
Services: 5
Receivers: 3
Providers: 4

Exported Activities: 1 Exported Services: 0 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=USA, L=USA, O=Usablenet, OU=Usablenet, CN=Mitja Sturm

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2010-01-27 22:50:40+00:00 Valid To: 2064-10-30 22:50:40+00:00

Issuer: C=US, ST=USA, L=USA, O=Usablenet, OU=Usablenet, CN=Mitja Sturm

Serial Number: 0x4b60c340 Hash Algorithm: sha1

md5: 1ec1f3297514f60d96c132f70fd8ffcb

sha1: 4fba2b57c7526e4f6fd24607ee32f7888ffbb981

sha256: 37bff7c0ee776177f0fdcb98bca438901149533e4cb82fbcfc948222cbc11050

sha512: 539282e276ef03ce595a9710123041ae25c56c0ce02123306c845484ef59ba0caaa3b8a2ec3871ae1785170e98713a5f453fa48a7e4611e4e66441697dcc42b8

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 9ff56b23ec882fab1b4f5b3f9be7f11caf33dc3df499c787fee96136e7e6c02b

Found 1 unique certificates

EXAMPLICATION PERMISSIONS

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
org.fidoalliance.uaf.permissions.FIDO_CLIENT	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network- based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

ক্লি APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS				
	FINDINGS	DETAILS			
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.TAGS check possible VM check			
	Compiler	r8			
	FINDINGS	DETAILS			
	Anti Debug Code	Debug.isDebuggerConnected() check			
classes2.dex	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check possible VM check			
	Compiler	r8 without marker (suspicious)			
classes3.dex	FINDINGS	DETAILS			
	Compiler	r8 without marker (suspicious)			

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.aetna.aetnabetterhealthmobile.MainActivity	Schemes: https://, Hosts: qamedicaid.aetna.com, medicaid.aetna.com, Path Prefixes: /MWP2/mobile, /MWP3/mobile, /MWP4/mobile, /MWP/mobile,

△ NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	App Link assetlinks.json file not found [android:name=com.aetna.aetnabetterhealthmobile.MainActivity] [android:host=https://qamedicaid.aetna.com]	high	App Link asset verification URL (https://qamedicaid.aetna.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 403). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	App Link assetlinks.json file not found [android:name=com.aetna.aetnabetterhealthmobile.MainActivity] [android:host=https://medicaid.aetna.com]	high	App Link asset verification URL (https://medicaid.aetna.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity (com.aetna.aetnabetterhealthmobile.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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: 0 | WARNING: 7 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/aetna/aetnabetterhealthmobile/AppLog.java com/aetna/aetnabetterhealthmobile/CustomAdapter.java com/aetna/aetnabetterhealthmobile/FirebaseMsgService.j ava com/aetna/aetnabetterhealthmobile/MainActivity.java com/aetna/aetnabetterhealthmobile/PinView.java

NO	ISSUE	SEVERITY	STANDARDS	com/aetna/aetnabetterhealthmobile/Utils.java
NO	ISSUE	SEVERITY	STANDARDS	
				com/hypr/hyprandroidcommon/App.java com/hypr/hyprandroidcommon/asm/AsmDataModel.java com/hypr/hyprandroidcommon/asm/AsmIntentManager.j ava com/hypr/hyprandroidcommon/asm/HyprBaseAsmActivit y.java com/hypr/hyprandroidcommon/authenticator/BasicTlvUti

NO	ISSUE	SEVERITY	STANDARDS	FILES pr/hyprandroidcommon/authenticator/HyprDbEn c.java
				com/hypr/hyprandroidcommon/authenticator/HyprPrefs.j
				ava
				com/hypr/hyprandroidcommon/authenticator/TlvProcess
				or.java
				com/hypr/hyprandroidcommon/authenticator/des/HyprC
				ustomDeserializer.java
				com/hypr/hyprandroidcommon/barcode/BarcodeParser.j
				ava
				com/hypr/hyprandroidcommon/barcode/barcode/Barcod
				eCaptureActivity.java
				com/hypr/hyprandroidcommon/barcode/mlkit/MlKitScan
				ningActivity.java
				com/hypr/hyprandroidcommon/barcode/ui/activities/Hyp
				rBarcodeActivity.java
				com/hypr/hyprandroidcommon/barcode/ui/camera/Cam
				eraSource.java
				com/hypr/hyprandroidcommon/barcode/ui/camera/Cam
				eraSourcePreview.java
				com/hypr/hyprandroidcommon/crypto/HMAC.java
				com/hypr/hyprandroidcommon/crypto/OfflineMode.java
				com/hypr/hyprandroidcommon/exceptions/HyprExceptio
				n.java
				com/hypr/hyprandroidcommon/fido2/HyprFido2.java
				com/hypr/hyprandroidcommon/fido2/HyprFido2Biometri
				cPromptAdapter.java
				com/hypr/hyprandroidcommon/fido2/setBiometricCapab
				le.java
				com/hypr/hyprandroidcommon/fidoclient/client/HyprBas
				eClientActivity.java
				com/hypr/hyprandroidcommon/fidoclient/client/HyprFid
				oClientAdapterResetActivity.java
				com/hypr/hyprandroidcommon/fidoclient/client/IntentMa
				nagerClient.java
				com/hypr/hyprandroidcommon/fidoclient/client/IntentTy
				7. 7.
				peDiscover.java
				com/hypr/hyprandroidcommon/fidoclient/client/IntentTy
				peOperation.java
				com/hypr/hyprandroidcommon/fidoclient/client/Operatio
				nManagerBase.java
				com/hypr/hyprandroidcommon/fidoclient/client/PolicyMa
				tcher.java

NIO	ICCLIE	CEVEDITY.	CTANDARDC	com/hypr/hyprandroidcommon/fidoclient/client/TrustedF
NO	ISSUE	SEVERITY	STANDARDS	File: Sapter.java
				com/hypr/hyprandroidcommon/fidoclient/model/ClientD
				ataModel.java
				com/hypr/hyprandroidcommon/fidoclient/ui/chooseaaid/
				ChooseAaidFragment.java
				com/hypr/hyprandroidcommon/fidomodel/BaseJsonObje
				ct.java com/hypr/hyprandroidcommon/relyingpartyadapter/Base
				FidoRelyingPartyAdapter.java
				com/hypr/hyprandroidcommon/relyingpartyadapter/Hea
				derInterceptor.java
				com/hypr/hyprandroidcommon/relyingpartyadapter/Hyp
				rRPA.java
				com/hypr/hyprandroidcommon/relyingpartyadapter/Retr
				ofitGenerator.java
				com/hypr/hyprandroidcommon/trust/data/HyprTeeKeyTy
				pe.java
				com/hypr/hyprandroidcommon/ui/activities/HyprBaseAct
				ivity.java
				com/hypr/hyprandroidcommon/ui/activities/HyprDeregis
				terAaidsActivity.java
				com/hypr/hyprandroidcommon/ui/activities/HyprGetRegi
				strationsAaidsActivity.java
				com/hypr/hyprandroidcommon/ui/observers/HyprLifecyc
				leObserver.java
				com/hypr/hyprandroidcommon/uiadapter/adapters/Hypr
				ActionAdapter.java
				com/hypr/hyprandroidcommon/uiadapter/adapters/Hypr
				Actions.java
				com/hypr/hyprandroidcommon/uiadapter/adapters/Hypr
				App.java
				com/hypr/hyprandroidcommon/uiadapter/ui/activities/H
				yprActionActivity.java
				com/hypr/hyprandroidcommon/uiadapter/ui/config/Hypr
				ColorConfig.java
				com/hypr/hyprandroidcommon/uiadapter/ui/config/Hypr
				ImageConfig.java
				com/hypr/hyprandroidcommon/uiadapter/ui/config/Hypr
				StringConfig.java
				com/hypr/hyprandroidcommon/uiadapter/ui/screens/cert
				retrieve/HyprCertRetrieveProgressFragment.java
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive	com/hypr/hyprandroidcommon/uiadapter/ui/screens/dev options/HyprDevOptionsFragment.iava
1	THE ADD 108S INFORMATION. SENSITIVE	ı ı		EVEI:10H9M3P14SH0DI0OAATIONALIGNA

chine/hypr/haprandroidcommon/udaqater/ui/screens/machine/delete/HyprDeleteMachineProgressPresenter_java com/hypr/hyprandroidcommon/udaqater/ui/screens/machine/license/HyprOoblicensepbeviceSetupMachineProgressFresenter_java com/hypr/hypronduroidcommon/udaqater/ui/screens/machine/license/HyprOoblicensepbeviceSetupMachineProgressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/machine/license/HyprOoblicenseDeviceSetupMachineProgressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressPragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressFragment_java com/hypr/hyprandroidcommon/udaqater/ui/screens/progressFragment_java com/hypr/hyprandroidcommon/useragent/Hypr/ul/screens/progressFragment_java com/hypr/hyprandroidcommon/useragent/Hypr/ul/screens/progressFragment_java com/hypr/hyprandroidcommon/useragent/data/Hypr/ul/screens/progressFragment_java com/hypr/hyprandroidcommon/useragent/data/Hypr/DataModel_java com/hypr/hyprandroidcommon/useragent/data/Hypr/DataModel_java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rfStatus/Result_java	NO	information should never be logged. ISSUE	severity	Information into Log File STVANTUARYSSMSTG-STORAGE-3	com/hypr/hyprandroidcommon/uiadapter/ui/screens/lice FILES hsepintestmode/HyprLicensePinTestModePresenter.java
com/hypr/hyprandroidcommon/useragent/data/profiles/ HyprAppProfile.java					com/hypr/hyprandroidcommon/uiadapter/ui/screens/ma chine/HyprMachineProgressPresenter.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/ma chine/delete/HyprDeleteMachineProgressPresenter.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/ma chine/license/HyprOobLicenseDeviceSetupMachineProgre ssFragment.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/ma chine/license/HyprOobLicenseDeviceSetupMachineProgre ssPresenter.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/pin single/HyprSinglePinFragment.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/pro gress/HyprProgressFragment.java com/hypr/hyprandroidcommon/uiadapter/ui/screens/pro gress/HyprPogressFragment.java com/hypr/hyprandroidcommon/uiadapter/ui/views/Custo mToolbar.java com/hypr/hyprandroidcommon/useragent/HyprUafUserA gent.java com/hypr/hyprandroidcommon/useragent/HyprUserAgen tOperation.java com/hypr/hyprandroidcommon/useragent/data/BaseData.java com/hypr/hyprandroidcommon/useragent/data/HyprDat aModel.java com/hypr/hyprandroidcommon/useragent/data/appprop erties/HyprEvents.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rStatusResult.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRemoteDevice.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRemoteDevice.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRemoteDevice.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRemoteDevice.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRemoteDevice.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rRessionData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rSessionData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rSessionData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rUafFidoData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rUafFidoData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rUafFidoData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rUafFidoData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rUafFidoData.java co

10	ISSUE	SEVERITY	STANDARDS	HyprApperonies.java ငှရကုင်လျှာr/hyprandroidcommon/useragent/data/pushnoti
10	13301	JE V LIXII I	SIANDANDS	fications/HyprPnaData.java
				com/hypr/hyprandroidcommon/useragent/data/user/acc
				ount/HyprAccountData.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/fidocl
				ientadapter/HyprFCAActivityProcessor.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/fidocl
				ientadapter/HyprFidoClientManager.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/fidocl
				ientadapter/setAdvertiseUdpBroadcast.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/fidop
				ayloadadapter/HyprFPA.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/AuthenticateOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/AuthenticationCancelOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/BaseOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/DeregisterOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/FeaturesOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/GetRegistrationsOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/operations/MachineStatusOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/OobLicenseDeviceSetupOperationV2.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/OobMagicLinkOperationV4.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/OobRpDeviceRegistrationOperationV2.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/OobRpDeviceSetupOperationV2.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/PendingAuthenticationCheckOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/RegisterOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/RegistrationCancelOperation.java
				com/hypr/hyprandroidcommon/useragent/fido/uaf/opera
				tions/UpdatePushTokenOperation.java
		1		com/hypr/hyprandroidcommon/useragent/fido/uaf/opera

NO	ISSUE	SEVERITY	STANDARDS	tions/WebsiteDeregisterOperation.java HbESypr/hyprandroidcommon/useragent/fido/uaf/opera
NO	ISSUE	SEVERITY	STANDARDS	FilhFbypr/hyprandroidcommon/useragent/fido/uaf/operations/WorkstationDeregisterOperation.java com/hypr/hyprandroidcommon/useragent/fido/uaf/operations/WorkstationLockOperation.java com/hypr/hyprandroidcommon/useragent/fido/uaf/operations/WorkstationUnlockCancelOperation.java com/hypr/hyprandroidcommon/useragent/fido/uaf/operations/WorkstationUnlockCompleteOperationV2.java com/hypr/hyprandroidcommon/useragent/fido/uaf/operations/WorkstationUnlockOperation.java com/hypr/hyprandroidcommon/useragent/fido/uaf/ops/BaseBackgroundOp.java com/hypr/hyprandroidcommon/useragent/fido/uaf/ops/BaseForegroundOp.java com/hypr/hyprandroidcommon/useragent/fido/uaf/ops/CertRetrievalOp.java com/hypr/hyprandroidcommon/useragent/fido/uaf/ops/LogSubmissionOp.java com/hypr/hyprandroidcommon/useragent/fido/uaf/ops/RegistrationCancelBackgroundOp.java com/hypr/hyprandroidcommon/utils/Base64url.java com/hypr/hyprandroidcommon/utils/HyprConformanceLogger.java com/hypr/hyprandroidcommon/utils/HyprDGUtils.java com/hypr/hyprandroidcommon/utils/HyprDGUtils.java com/hypr/hyprandroidcommon/utils/HyprDg.java com/hypr/hyprandroidcommon/utils/HyprDg.java com/hypr/hyprandroidcommon/utils/HyprSupportLog.java com/hypr/hyprandroidcommon/utils/HyprSupportLog.java com/hypr/hyprandroidcommon/utils/HyprSupportLog.java
				com/hypr/hyprandroidfingerprintframework/model/data/
				mAuthenticators.java com/hypr/hyprandroidpinframework/ui/activities/HyprPi nActivity.java com/hypr/hyprandroidpinframework/ui/screens/pinentry /pinsingle/HyprPinSingleVerifyScreenReaderEnabledFrag
				ment.java com/hypr/hyprandroidpresence/model/HyprAsmAuthenti cators.java com/hypr/hyprandroidpresence/ui/activities/HyprPresenc

NO	ISSUE	SEVERITY	STANDARDS	com/hypr/hyprandroidsilent/model/HyprAsmAuthenticat FILES ors.Java
				net/danlew/android/joda/ResUtils.java net/danlew/android/joda/TimeZoneChangedReceiver.java org/joda/time/tz/DateTimeZoneBuilder.java timber/log/Timber.java
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	com/aetna/model/Constants.java com/aetna/webservice/RBATokenAsync.java com/appdynamics/eumagent/runtime/Instrumentation.ja va com/cvshealth/ngasdk/data/config/NgaConfig.java com/cvshealth/ngasdk/data/environment/NgaConstants.j ava com/cvshealth/ngasdk/data/environment/NgaEnvironme nt.java com/cvshealth/ngasdk/data/misc/RequestUtilsImpl.java com/cvshealth/ngasdk/domain/model/config/BasicAuth.ja va com/cvshealth/ngasdk/domain/model/config/Key.java com/cvshealth/ngasdk/domain/model/config/OAuth2.jav a com/cvshealth/ngasdk/domain/model/persistance/Persist enceObj.java com/hypr/crypto/TrustedCommandException.java com/hypr/crypto/TrustedCommandException.java com/hypr/hyprandroidcommon/barcode/BarcodeParserK t.java com/hypr/hyprandroidcommon/useragent/data/datastruc t/BaseFragmentData.java com/hypr/hyprandroidcommon/useragent/data/fido/Hyp rActivityResultData.java io/reactivex/internal/schedulers/SchedulerPoolFactory.jav a
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/appdynamics/eumagent/runtime/p000private/bf.jav a com/hypr/hyprandroidcommon/authenticator/HyprDbEn c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/hypr/hyprandroidcommon/asm/setBiometricCapabl e.java com/hypr/hyprandroidcommon/authenticator/setBiometr icCapable.java com/hypr/hyprandroidcommon/authenticator/setDevicel d.java com/hypr/hyprandroidcommon/crypto/setBiometricCapa ble.java com/hypr/hyprandroidcommon/fidoclient/client/setAdver tiseUdpBroadcast.java com/hypr/hyprandroidcommon/fidoclient/client/setBiom etricCapable.java com/hypr/hyprandroidcommon/relyingpartyadapter/setA dvertiseUdpBroadcast.java com/hypr/hyprandroidcommon/relyingpartyadapter/setB iometricConfigured.java com/hypr/hyprandroidcommon/relyingpartyadapter/setD elegate.java com/hypr/hyprandroidfingerprintframework/model/data/ isShowDebug.java com/hypr/hyprandroidpinframework/ui/screens/pinentry /pindouble/BuildConfig.java
5	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/aetna/aetnabetterhealthmobile/WebFragment.java com/hypr/hyprandroidcommon/utils/HyprConformanceL ogger.java com/hypr/hyprandroidcommon/utils/HyprSupportLog.jav a
6	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	com/hypr/hyprandroidcommon/authenticator/BasicTlvUti ls.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/appdynamics/eumagent/runtime/p000private/af.jav a com/appdynamics/eumagent/runtime/p000private/ai.jav a com/appdynamics/eumagent/runtime/p000private/aj.jav a
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/aetna/webservice/LoginHintAsync.java com/cvshealth/ngasdk/data/remote/service/RetrofitObj.ja va com/hypr/hyprandroidcommon/relyingpartyadapter/Retr ofitGenerator.java com/hypr/hyprandroidcommon/relyingpartyadapter/Retr ofitGeneratorAsync.java
9	This app has capabilities to prevent tapjacking attacks.	secure	OWASP MASVS: MSTG-PLATFORM-9	com/cvshealth/ngasdk/utils/NgaExtentionsKt.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/aetna/aetnabetterhealthmobile/WebFragment.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64- v8a/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86_64/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi- v7a/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64- v8a/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi- v7a/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libFido2Authenticator.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk']	True info Symbols are stripped.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION	
----	------------	-------------	---------	-------------	--

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR LABEL		FILES		
00096	Connect to a URL and set request method command network		com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java		
00123	Save the response to JSON after connecting to the remote server	network command	com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java		
00089	Connect to a URL and receive input stream from the server		com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java		
00030	Connect to the remote server through the given URL	network	com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java		

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java
00094	Connect to a URL and read data from it	command network	com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/LoginHintAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java
00108	Read the input stream from given URL	network command	com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/webservice/ApplicationTokenAsync.java com/aetna/webservice/NewApplicationTokenAsync.java com/aetna/webservice/RBATokenAsync.java com/aetna/webservice/UserTokenAsync.java
00013	Read file and put it into a stream	file	com/appdynamics/eumagent/runtime/p000private/aa.java com/appdynamics/eumagent/runtime/p000private/bl.java com/hypr/crypto/ADPContext.java com/hypr/crypto/ADPContextStorage.java com/hypr/crypto/CrustyContext.java com/hypr/crypto/ac.java com/hypr/crypto/asn1/j.java com/hypr/crypto/des/LegacyContextDeserializer.java okio/OkioJvmOkioKt.java org/joda/time/tz/ZoneInfoProvider.java
00022	Open a file from given absolute path of the file	file	com/aetna/aetnabetterhealthmobile/WebFragment.java com/appdynamics/eumagent/runtime/p000private/bl.java com/appdynamics/eumagent/runtime/p000private/e.java com/appdynamics/eumagent/runtime/p000private/x.java
00091	Retrieve data from broadcast	collection	com/aetna/aetnabetterhealthmobile/MainActivity.java com/aetna/aetnabetterhealthmobile/VerifyPINActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/aetna/aetnabetterhealthmobile/WebFragment.java com/aetna/versioncontrolnative/VersionController.java
00036	Get resource file from res/raw directory	reflection	com/aetna/versioncontrolnative/VersionController.java
00075	Get location of the device collection location		com/cvshealth/ngasdk/domain/usecase/ConfigurationInitObj.java
00115	Get last known location of the device collection location		com/cvshealth/ngasdk/domain/usecase/ConfigurationInitObj.java
00175	Get notification manager and cancel notification		com/aetna/aetnabetterhealthmobile/Utils.java
00183	Get current camera parameters and change the setting.	camera	com/hypr/hyprandroidcommon/barcode/ui/camera/CameraSource.java
00202	Make a phone call	control	com/aetna/aetnabetterhealthmobile/WebFragment.java
00203	Put a phone number into an intent	control	com/aetna/aetnabetterhealthmobile/WebFragment.java
00072	Write HTTP input stream into a file	command network file	com/aetna/aetnabetterhealthmobile/WebFragment.java
00024	Write file after Base64 decoding	reflection file	com/aetna/aetnabetterhealthmobile/WebFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/aetna/aetnabetterhealthmobile/WebFragment.java
00125	Check if the given file path exist	file	com/aetna/aetnabetterhealthmobile/WebFragment.java
00153	Send binary data over HTTP	http	com/aetna/aetnabetterhealthmobile/WebFragment.java



TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://aetna-better-health-f5f9b.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/683095936570/namespaces/firebase:fetch? key=AlzaSyBn5K8Q5OsfJA6IC7d8zpEi3KeOAhPyhYE. This is indicated by the response: {'state': 'NO_TEMPLATE'}

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

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

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
mobile.eum-appdynamics.com	ok	IP: 52.42.18.116 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
developer.android.com	ok	IP: 64.233.176.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
qaapi10.cvshealth.com	ok	IP: 45.223.17.220 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

DOMAIN	STATUS	GEOLOCATION
pay.google.com	ok	IP: 142.250.105.92 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
schemas.android.com	ok	No Geolocation information available.
image.eum-appdynamics.com	ok	IP: 54.201.185.97 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
aetna-better-health-f5f9b.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
licensing.hypr.com	ok	No Geolocation information available.
healthhist.com	ok	IP: 44.227.116.77 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

DOMAIN	STATUS	GEOLOCATION
qamedicaid.aetna.com	ok	IP: 23.62.226.177 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
healthhist.cvshealthfhirdev.com	ok	IP: 44.217.183.239 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
pdx-col.eum-appdynamics.com	ok	IP: 52.43.242.54 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
pdx-col-image.eum-appdynamics.com	ok	No Geolocation information available.

A TRACKERS

TRACKER	CATEGORIES	URL
Appdynamics	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/194

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

₽ HARDCODED SECRETS

POSSIBLE SECRETS
"file_provider_authority" : "com.aetna.aetnabetterhealthmobile.fileprovider"
"firebase_database_url" : "https://aetna-better-health-f5f9b.firebaseio.com"
"hypr_check_for_pending_auth_on_app_resume_override" : "FALSE"
"hypr_fido_client_choose_aaid_authenticate_shown_override" : "TRUE"
"hypr_fido_multi_auth_screen_enabled_override" : "TRUE"
"google_crash_reporting_api_key" : "AlzaSyBn5K8Q5OsfJA6lC7d8zpEi3KeOAhPyhYE"
"hypr_pin_show_auth_conf_override" : "false"
"hypr_presence_show_auth_conf_override" : "false"
"hypr_accept_authentication_fragment_class_override" : "NONE"
"hypr_contact_support_email_body_api" : "API: "
"google_api_key" : "AlzaSyBn5K8Q5OsfJA6IC7d8zpEi3KeOAhPyhYE"

POSSIBLE SECRETS

"AppD_Key" : "AD-AAB-ACS-KUU"

"hypr_fido_multi_auth_fragment_class_override" : "NONE"

DB7C2ABF62E35E668076BEAD2088

0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

E95E4A5F737059DC60DFC7AD95B3D8139515620F

POSSIBLE SECRETS 0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01

2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

74D59FF07F6B413D0EA14B344B20A2DB049B50C3

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

64033881142927202683649881450433473985931760268884941288852745803908878638612

04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD28 9A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F

FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD 65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94B B2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE 3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F77FE E598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D 5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E98E458857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135 C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A4 6B4DB5A851F444182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA44442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657 FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C35387E3BA00077D9B4763E4 E4894B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F55E62292C311562A846505DC82DB854338A E49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF 600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555BE7747C932665CB20C0F1CC01BD70229388839D2AF05E45450 4AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C866B022BB7099876A460E7451A8A93109703FEE1C217E6C382665CB2C0F1CC01BD70229388839D2AF05E45450 4AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C866B022BB7099876A460E77451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC999E9E31650C1217B6 24816CDAD9A95F9D5B8019488D90A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA

1E589A8595423412134FAA2DBDEC95C8D8675E58

0c14416e6f6e796d6f75732053656e64657220202020

04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

MQVwithSHA512KDFAndSharedInfo

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

04B8266A46C55657AC734CE38F018F2192

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03

883423532389192164791648750360308885314476597252960362792450860609699839

115792089210356248762697446949407573529996955224135760342422259061068512044369

2866537B676752636A68F56554E12640276B649EF7526267

29818893917731240733471273240314769927240550812383695689146495261604565990247

00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3

3045AE6FC8422F64ED579528D38120EAE12196D5

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969ED
B767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD2
07A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82
A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

POSSIBLE SECRETS 0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00 00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E 5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B 07A526C63D3E25A256A007699F5447E32AE456B50E 7503CFE87A836AF3A61B8816F25450F6CF5F1C93ACF1ABC1778064FDCBFFA921DF1626BF4FD036F93D75F6A50F3A41F98028FF5FC235F5B889A589CB5215F2A4 0307AF69989546103D79329FCC3D74880F33BBE803CB 04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE 65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94B B2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE 3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7E E598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D 5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135 C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A4 6B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFF 790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16 3045AE6FC8422f64ED579528D38120EAE12196D5 00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A 10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF

64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

POSSIBLE SECRETS 0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D 0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7 FFFFFFF00000000FFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551 0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8 00F50B028E4D696E676875615175290472783FB1 fffffff00000000ffffffffffffffbce6faada7179e84f3b9cac2fc632551 9494fec095f3b85ee286542b3836fc81a5dd0a0349b4c239dd38744d488cf8e31db8bcb7d33b41abb9e5a33cca9144b1cef332c94bf0573bf047a3aca98cdf3b C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8 FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C5 5DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7 DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BA D946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBB C2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDD C186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFF 662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04 B4E134D3FB59EB8BAB57274904664D5AF50388BA 02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7 040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883 2AA058F73A0E33AB486B0F610410C53A7F132310 4099B5A457F9D69F79213D094C4BCD4D4262210B

POSSIBLE SECRETS
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
7d7374168ffe3471b60a857686a19475d3bfa2ff
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
985BD3ADBAD4D696E676875615175A21B43A97E3
6db14acc9e21c820ff28b1d5ef5de2b0
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
3086d221a7d46bcde86c90e49284eb15
b8adf1378a6eb73409fa6c9c637ba7f5
9760508f15230bccb292b982a2eb840bf0581cf5
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
010092537397ECA4F6145799D62B0A19CE06FE26AD
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402 8291115057151
E95E4A5F737059DC60DF5991D45029409E60FC09
10E723AB14D696E6768756151756FEBF8FCB49A9

POSSIBLE SECRETS
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FE EC5864E19C054FF99129280E4646217791811142820341263C5315
153d5d6172adb43045b68ae8e1de1070b6137005686d29d3d73a7749199681ee5b212c9b96bfdcfa5b20cd5e3fd2044895d609cf9b410b7a0f12ca1cb9a428cc
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
6b8cf07d4ca75c88957d9d670591
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
98b1413a-2420-4d2e-9cd4-8f558856aa2b
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
3086d221a7d46bcde86c90e49284eb153dab
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
sha256/dF9hP3SndbQA+P2WilYxj2lpU5H5t1G0WJdhxX8VTk4=
sha256/HQV0P8Q4ERKl8kPZvK6440pc451clTnrSLOuvwWpxKg=
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

4D696E676875615175985BD3ADBADA21B43A97E2

A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7FBD7D3B9A9 2EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5

0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311

020A601907B8C953CA1481EB10512F78744A3205FD

1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF 6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C7 06C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7 B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

71169be7330b3038edb025f1

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975

AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E9

0B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335

E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE1

9DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A2979962

0F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177D D2259

00E8BEE4D3E2260744188BE0E9C723

1340780792994259709957402499820584612747936582059239337772356144372176403007354697680187429816690342769003185818648605085375388281194656994643364906084095

 $133531813272720673433859519948319001217942375967847486899482359599369642528734712461590403327731821410328012529253871914788598993103310567744136\\196364803064721377826656898686468463277710150809401182608770201615324990468332931294920912776241137878030224355746606283971659376426832674269780\\880061631528163475887$

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E788
0E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34
E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE53
8175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE
13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91
328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

B99B99B099B323E02709A4D696E6768756151751

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

79885141663410976897627118935756323747307951916507639758300472692338873533959

90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D

POSSIBLE SECRETS
28792665814854611296992347458380284135028636778229113005756334730996303888124
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065
D6031998D1B3BBFEBF59CC9BBFF9AEE1
115792089237316195423570985008687907853269984665640564039457584007913129639316
b3fb3400dec5c4adceb8655d4c94
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
24B7B137C8A14D696E6768756151756FD0DA2E5C
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
10B7B4D696E676875615175137C8A16FD0DA2211
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
6b8cf07d4ca75c88957d9d67059037a4

POSSIBLE SECRETS
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
115792089237316195423570985008687907853073762908499243225378155805079068850323
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
401028774D7777C7B7666D1366EA432071274F89FF01E718
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D 566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
6277101735386680763835789423207666416083908700390324961279
db92371d2126e9700324977504e8c90e
659EF8BA043916EEDE8911702B22
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

POSSIBLE SECRETS
03E5A88919D7CAFCBF415F07C2176573B2
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A 01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD 4C143EF1C7A3
D2C0FB15760860DEF1EEF4D696E6768756151754
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
MQVwithSHA256KDFAndSharedInfo
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
85E25BFE5C86226CDB12016F7553F9D0E693A268
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
340282366920938463463374607431768211455

POSSIBLE SECRETS 04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985 D09E8800291CB85396CC6717393284AAA0DA64BA 145188775577763990151158743208307020242261438098488931355057091965931517706595657435907891265414916764399268423699130577757433083166651158914570 105971074227669275788291575622090199821297575654322355049043101306108213104080801056529374892690144291505781966373045481835947239164288532817130 2299245556663073719855 005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2 6BA06FE51464B2BD26DC57F48819BA9954667022C7D03

520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6

e43bb460f0b80cc0c0b075798e948060f8321b7d

7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9

0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475 B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928

C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95EC
A1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33
EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418D
E8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83

0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AA
AC6AC7D35245D1692E8EE1

00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814

00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9

023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd

517cc1b727220a94fe13abe8fa9a6ee0

7A1F6653786A68192803910A3D30B2A2018B21CD54

sha256/LeM8XnCly8+Cxm+HKTEOBZr1g3D8odQNHTH+vdu7RWc=

70390085352083305199547718019018437840920882647164081035322601458352298396601

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b10 22c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C209E0C64975
17ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63ACAE1CAA6B7902D5252
6735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857F689962856DED4010ABD0BE621C
3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597

0217C05610884B63B9C6C7291678F9D341

021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F

6C01074756099122221056911C77D77E77A777E7E7E77FCB

115792089210356248762697446949407573530086143415290314195533631308867097853951

POSSIBLE SECRETS
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280 8892707005449
4A6E0856526436F2F88DD07A341E32D04184572BEB710
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
7fffffffffffffffffffffffffffffffffffff
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
0340340340340340340340340340340340340340
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C 8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4 827AF1B8AC15B

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

POSSIBLE SECRETS
0095E9A9EC9B297BD4BF36E059184F
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
28091019353058090096996979000309560759124368558014865957655842872397301267595
sha256/++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1al=
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
115792089237316195423570985008687907853269984665640564039457584007913129639319
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B461 54D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
115792089237316195423570985008687907853269984665640564039457584007913129639935
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
91771529896554605945588149018382750217296858393520724172743325725474374979801
96341f1138933bc2f503fd44

 $142011741597563481196368286022318089743276138395243738762872573441927459393512718973631166078467600360848946623567625795282774719212241929071046\\134208380636394084512691828894000571524625445295769349356752728956831541775441763139384457191755096847107846595662547942312293338483924514339614\\727760681880609734239$

A335926AA319A27A1D00896A6773A4827ACDAC73

1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10

0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500

6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a

c469684435deb378c4b65ca9591e2a5763059a2e

340E7BE2A280EB74E2BE61BADA745D97E8F7C300

68363196144955700784444165611827252895102170888761442055095051287550314083023

7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E

0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205

040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C34 60782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

000E0D4D696E6768756151750CC03A4473D03679

470fa2b4ae81cd56ecbcda9735803434cec591fa

F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F

7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA

POSSIBLE SECRETS
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
429418261486158041438734477379555023926723459686071430667981129940894712314200270603852166995638487199576572848148989097707594626134376694563648 827303708389347910808359326479767786019153434744009610342313166725786869204821949328786333602033847970926843422476210557602350161326147806527610 28509445403338652341
114ca50f7a8e2f3f657c1108d9d44cfd8
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
DB7C2ABF62E35E7628DFAC6561C5
07A11B09A76B562144418FF3FF8C2570B8
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
MQVwithSHA384KDFAndSharedInfo
072546B5435234A422E0789675F432C89435DE5242
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
22123dc2395a05caa7423daeccc94760a7d462256bd56916

9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC 67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442 734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB

04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9

0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B

03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

57896044618658097711785492504343953927102133160255826820068844496087732066703

1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD5 95F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DB88BACE198B61E00F8B332

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

F518AA8781A8DF278ABA4E7D64B7CB9D49462353

DB7C2ABF62E35E668076BEAD208B

POSSIBLE SECRETS
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
12511cfe811d0f4e6bc688b4d
002757A1114D696E6768756151755316C05E0BD4
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
100997906755055304772081815535925224869841082572053457874823515875577147990529272777244152852699298796483356699682842027972896052747173175480590 485607134746852141928680912561502802222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588 322876850946740663962
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
31a92ee2029fd10d901b113e990710f0d21ac6b6
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
57896044618658097711785492504343953926634992332820282019728792003956564823190
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D

POSSIBLE SECRETS
127971af8721782ecffa3
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
7B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
sha256/FhyOXTiTcqoqreRDxlLFerO4lK1rnbaUOEz9SpOoFoo=
b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046
51DEF1815DB5ED74FCC34C85D709
1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de
3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F62901228F8C28 CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045AF2767164E1DFC967C 1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353BBB64E0EC377FD028370DF92B52C 7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1
5FF6108462A2DC8210AB403925E638A19C1455D21

POSSIBLE SECRETS
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
115792089237316195423570985008687907853269984665640564039457584007913129639936
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
003088250CA6E7C7FE649CE85820F7
FFFFFFE0000000075A30D1B9038A115
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
5EEEFCA380D02919DC2C6558BB6D8A5D
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7 636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706

POSSIBLE SECRETS
5F49EB26781C0EC6B8909156D98ED435E45FD59918
c49d360886e704936a6678e1139d26b7819f7e90
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
71169be7330b3038edb025f1d0f9
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
1243ae1b4d71613bc9f780a03690e
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE5E9001A8D 66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D119529A45D6F834566E3025 E316A330EFBB77A86F0C1AB15B051AE3D428C8F8ACB70A8137150B8EEB10E183EDD19963DDD9E263E4770589EF6AA21E7F5F2FF381B539CCE3409D13CD566AFBB48D6C01918 1E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
6EE3CEEB230811759F20518A0930F1A4315A827DAC
57896044618658097711785492504343953926634992332820282019728792003956564823193
9162fbe73984472a0a9d0590
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955 727A
004D696E67687561517512D8F03431FCE63B88F4
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a 3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
e8b4011604095303ca3b8099982be09fcb9ae616
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839 296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650

POSSIBLE SECRETS
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
416E6F6E796D6F75732053656E64657220202020
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
sha256/5kJvNEMw0KjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
6127C24C05F38A0AAAF65C0EF02C
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
4E13CA542744D696E67687561517552F279A8C84
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66D3F8152AD 6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A317091883681286130BC8985DB1602 E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60E69CC928B2B9C52172E413042E9 B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F

10C0FB15760860DEF1EEF4D696E676875615175D

103FAEC74D696E676875615175777FC5B191EF30

c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

340282366920938463463374607431768211456

B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFACCBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371

1053CDE42C14D696E67687561517533BF3F83345

C49D360886E704936A6678E1139D26B7819F7E90

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC

D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

e4437ed6010e88286f547fa90abfe4c42212

POSSIBLE SECRETS 02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7 0108B39E77C4B108BED981ED0E890E117C511CF072 0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45B E8112F4 026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D 801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB 70390085352083305199547718019018437841079516630045180471284346843705633502619 sha256/MBy3UQV+C68BgihaLTDj1vHRGIj+2SUC0Tzxa70Zx2Y= 0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1 E87579C11079F43DD824993C2CEE5ED3 36DF0AAFD8B8D7597CA10520D04B 127021248288932417465907042777176443525787653508916535812817507265705031260985098497423188333483401180925999995120988934130659205614996724254121 883686778842537820383 139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740 747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803 187341288580489525163 00689918DBEC7E5A0DD6DFC0AA55C7

036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a

POSSIBLE SECRETS
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D 1EE71B1B9BC0455FB0D2C3
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
E95E4A5F737059DC60DFC7AD95B3D8139515620C
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
70390085352083305199547718019018437841079516630045180471284346843705633502616
134078079299425970995740249982058461274793658205923933777235614437217640300735469768018742981669034276900318581864860508537538828119465699464336 49006084096

C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8 FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C5 5DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7 DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BA D946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBB C2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988DBFDD C186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B08 65A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55 E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32 806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12F EE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB 8BEFC848AD92222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82D DF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5E E382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53

4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9F265DF9FB240F



> PLAYSTORE INFORMATION

Title: Aetna Better Health - Medicaid

Score: 3.34 Installs: 100,000+ Price: 0 Android Version Support: Category: Medical Play Store URL: com.aetna.aetnabetterhealthmobile

Developer Details: Aetna Inc, Aetna+Inc, None, http://www.aetnabetterhealth.com/app, mobiledevelopment@aetna.com,

Release Date: Feb 11, 2015 Privacy Policy: Privacy link

Description:

Aetna Better Health is an easy app for Medicaid members of Aetna Better Health to access their health care information and services. As an Aetna Better Health Medicaid member,

you may use the app to: • Find or change your provider • View your medical and prescription claims • View your current medications o View your benefits o Set up a new account which may be used for both mobile and web • Connect with the health plan through your secure inbox to: o Request an ID card o Request a change in PCP One more of your Aetna Better Health benefits - now available as a mobile app! NOTE: Aetna commercial members looking to access their health plan or search for network doctors can find this information by downloading the Aetna Mobile App.

∷ SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:06:43	Generating Hashes	ОК
2025-08-29 19:06:43	Extracting APK	ОК
2025-08-29 19:06:43	Unzipping	ОК
2025-08-29 19:06:44	Parsing APK with androguard	ОК
2025-08-29 19:06:44	Extracting APK features using aapt/aapt2	ОК
2025-08-29 19:06:44	Getting Hardcoded Certificates/Keystores	ОК
2025-08-29 19:06:47	Parsing AndroidManifest.xml	ОК
2025-08-29 19:06:47	Extracting Manifest Data	ОК

2025-08-29 19:06:47	Manifest Analysis Started	OK
2025-08-29 19:06:48	Reading Network Security config from network_security_config.xml	ОК
2025-08-29 19:06:48	Parsing Network Security config	OK
2025-08-29 19:06:48	Performing Static Analysis on: Aetna Better Health - Medicaid (com.aetna.aetnabetterhealthmobile)	OK
2025-08-29 19:06:49	Fetching Details from Play Store: com.aetna.aetnabetterhealthmobile	OK
2025-08-29 19:06:49	Checking for Malware Permissions	ОК
2025-08-29 19:06:49	Fetching icon path	ОК
2025-08-29 19:06:49	Library Binary Analysis Started	OK
2025-08-29 19:06:49	Analyzing lib/arm64-v8a/libFido2Authenticator.so	OK
2025-08-29 19:06:49	Analyzing lib/x86_64/libFido2Authenticator.so	ОК
2025-08-29 19:06:49	Analyzing lib/armeabi-v7a/libFido2Authenticator.so	ОК

2025-08-29 19:06:49	Analyzing lib/x86/libFido2Authenticator.so	ОК
2025-08-29 19:06:49	Analyzing apktool_out/lib/arm64-v8a/libFido2Authenticator.so	OK
2025-08-29 19:06:49	Analyzing apktool_out/lib/x86_64/libFido2Authenticator.so	OK
2025-08-29 19:06:49	Analyzing apktool_out/lib/armeabi-v7a/libFido2Authenticator.so	OK
2025-08-29 19:06:49	Analyzing apktool_out/lib/x86/libFido2Authenticator.so	OK
2025-08-29 19:06:49	Reading Code Signing Certificate	OK
2025-08-29 19:06:50	Running APKiD 2.1.5	OK
2025-08-29 19:06:54	Detecting Trackers	ОК
2025-08-29 19:06:57	Decompiling APK to Java with JADX	OK
2025-08-29 19:07:21	Converting DEX to Smali	OK
2025-08-29 19:07:22	Code Analysis Started on - java_source	OK

2025-08-29 19:07:24	Android SBOM Analysis Completed	ОК
2025-08-29 19:07:30	Android SAST Completed	ОК
2025-08-29 19:07:30	Android API Analysis Started	OK
2025-08-29 19:07:34	Android API Analysis Completed	ОК
2025-08-29 19:07:35	Android Permission Mapping Started	ОК
2025-08-29 19:07:39	Android Permission Mapping Completed	ОК
2025-08-29 19:07:39	Android Behaviour Analysis Started	ОК
2025-08-29 19:07:44	Android Behaviour Analysis Completed	ОК
2025-08-29 19:07:44	Extracting Emails and URLs from Source Code	ОК
2025-08-29 19:07:47	Email and URL Extraction Completed	OK
2025-08-29 19:07:47	Extracting String data from APK	OK

2025-08-29 19:07:48	Extracting String data from SO	OK
2025-08-29 19:07:48	Extracting String data from Code	OK
2025-08-29 19:07:48	Extracting String values and entropies from Code	OK
2025-08-29 19:07:54	Performing Malware check on extracted domains	OK
2025-08-29 19:07:56	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.