MOBSF

ANDROID STATIC ANALYSIS REPORT

Home (3.30.1.6)

File Name: com.google.android.apps.chromecast.app.apk

Package Name:	com.google.android.apps.chromecast.app
Scan Date:	Jan. 3, 2026, 6:05 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	52	3	4	2

FILE INFORMATION

File Name: com.google.android.apps.chromecast.app.apk
Size: 27.64MB
MD5: ef3419cd44e8a8ddf575a1133977fde1
SHA1: 5d8c5ae5ae31a48b0e7d944a85ff891f8c5bdbea
SHA256: 28f575a03a05698b53438535c2c20d82fc38b0331268c2ed46aa78c141b7e3e5

APP INFORMATION

App Name: Home
Package Name: com.google.android.apps.chromecast.app
Main Activity: com.google.android.apps.chromecast.app.homemanagement.settings.HomeSettingsActivity
Target SDK: 35
Min SDK: 28
Max SDK:
Android Version Name: 3.30.1.6
Android Version Code: 30484712

APP COMPONENTS

Activities: 195

Services: 23
Receivers: 35
Providers: 8
Exported Activities: 11
Exported Services: 5
Exported Receivers: 19
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: None
X.509 Subject: C=US, ST=CA, L=Mountain View, O=Google, Inc, OU=Google, Inc, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-12-02 02:07:58+00:00
Valid To: 2036-04-19 02:07:58+00:00
Issuer: C=US, ST=CA, L=Mountain View, O=Google, Inc, OU=Google, Inc, CN=Unknown
Serial Number: 0x4934987e
Hash Algorithm: md5
md5: d046fc5d1fc3cd0e57c5444097cd5449
sha1: 24bb24c05e47e0aefa68a58a766179d9b613a600
sha256: 3d7a1223019aa39d9ea0e3436ab7c0896bfb4fb679f4de5fe7c23f326c8f994a
sha512: 696a69f617980d711da35cce1fe6bddf2f3b76714d51758c5d1cef8f28eb3033371561c693c0819a57d07391a8cde08c99c92688c962252ffab21297e2df8e8e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 516ad3a6ae407da983ae7fd992217217ef8b7959a0d1711546a7dcc67f8e7460
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.apps.chromecast.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.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
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
com.google.android.apps.nest.DOCK_MANAGER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
com.google.android.apps.nest.CAST_AUTH_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.settings.setup.dock.RUN_DOCK_SETUP	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.apps.aicore.service.BIND_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.apps.chromecast.app.deeplink.DeeplinkActivity	Schemes: googlehome://, http://, Hosts: automations, device, controller, devices, structures, invite-to-structure, nest-aware, signup, setup, fsi, atriumFileViewer, appdownload, settings, homeview, feed, history, camera_immersive, camera_event, wifi, com.google.android.apps.chromecast.app, creategroup, sharesheet, partner, webview, favorites, safety, smokeco, assistant, homeagent, Path Prefixes: /help-me-create, /remotecontrol, /non-payer, /hanging-subscriptions, /3p-hanging-subscriptions, /event-video-history, /play-iap, /play-iap-management, /play-iap-catalog, /nest-aware, /hanging-sub-intro, /homeroutines/haw, /homeroutines/haw-mini, /device/, /nest-aware/hanging-subscription-apply, /duo_account, /ha_linking, /interconnect, /gal, /smartring, /feedback, /primary-network-settings, /station-list, /family-wifi, /migration, /unifiedSettings, /invite, /invite/review, /garageDoorCameraPlacementGuide, /alarm, /category, /nestprotect/migration, /share-password, /ghp, /test-network-speed, /prioritize-device,
com.google.android.apps.chromecast.app.DiscoveryActivity	Schemes: comgooglecast://, https://, googlehome://, http://, Hosts: chromecast.com, madeby.google.com, home.google.com, camera, g.co, email-prefs, Paths: /get-app/watch, /get-app/watch/, /get-app/discover, /get-app/discover/, /home-app, /home-app/, /home/app/, Path Prefixes: /migration, /nest_hub_max_setup,
com.google.android.apps.chromecast.app.deeplink.InternalDeeplinkActivity	Schemes: googlehome://, Hosts: assistantkit, setup, Path Prefixes: /discovery/matter,
com.google.android.apps.chromecast.app.deeplink.InternalDoorbellDeeplinkActivity	Schemes: googlehome://, Hosts: doorbell_event,
com.google.android.apps.chromecast.app.deeplink.ExternalDoorbellDeeplinkActivity	Schemes: googlehome://, Hosts: doorbell_event,
com.google.android.apps.chromecast.app.mediaapps.OAuthHandoffActivity	Schemes: comgooglecast://, Hosts: chromecast.auth.com, offers, Path Patterns: /done, /end,

ACTIVITY	INTENT
com.google.android.libraries.accountlinking.activity.AccountLinkingActivity	Schemes: comgooglecast://, https://, Hosts: galredirect, oauth-redirect.googleusercontent.com, Path Prefixes: /a/com.google.android.apps.chromecast.app,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	android.com appspot.com firebaseio.com g.co goo.gl google-analytics.com googleapis.com google.com gstatic.com nest.com nestlabs.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 41 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
5	Content Provider (com.google.android.libraries.home.notifications.fable.CameraPreviewProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.google.android.apps.chromecast.app.deeplink.DeeplinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity-Alias (com.google.android.apps.chromecast.app.DiscoveryActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity-Alias (com.google.android.apps.chromecast.app.deeplink.ExternalDoorbellDeeplinkActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.google.android.apps.chromecast.app.gf.maintenance.GeofenceSystemChangeBroadcastReceiver) 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.
10	Broadcast Receiver (com.google.android.apps.chromecast.app.gf.repository.GeofenceTransitionBroadcastReceiver) 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
11	TaskAffinity is set for activity (com.google.android.apps.chromecast.app.learn.LearnMediaBrowserActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
12	TaskAffinity is set for activity (com.google.android.apps.chromecast.app.learn.LearnMediaPlayerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
13	TaskAffinity is set for activity (com.google.android.apps.chromecast.app.learn.LearnTutorialCompleteActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
14	Activity (com.google.android.apps.chromecast.app.mediaapps.OAuthHandoffActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Broadcast Receiver (com.google.android.apps.chromecast.app.remotecontrol.safety.LockProximityReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BLUETOOTH|android.permission.BLUETOOTH_ADMIN [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.
16	Activity (com.google.android.apps.chromecast.app.setup.discovery.packages.matter.proxy.MatterSetupProxyActivity) 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.
17	Activity (com.google.android.apps.chromecast.app.systemcontrol.panel.GoogleHomePanelActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CONTROLS [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. 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
18	Service (com.google.android.apps.chromecast.app.systemcontrol.HomeControlService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CONTROLS [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.
19	Activity (com.google.android.apps.chromecast.app.titan.dock.activity.FirstDockActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.settings.setup.dock.RUN_DOCK_SETUP [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. 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
20	Broadcast Receiver (com.google.android.apps.chromecast.app.titan.dock.event.DockEventReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.INTERNAL_BROADCAST [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.
21	Broadcast Receiver (com.google.android.apps.chromecast.app.util.phenotype.PhenotypeBroadcastReceiver) 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.
22	Broadcast Receiver (com.google.android.apps.chromecast.app.whc.wifi.WifiChangedImplicitBroadcastReceiver) 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
23	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.
24	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
25	Activity (com.google.android.libraries.accountlinking.activity.AccountLinkingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
26	Broadcast Receiver (com.google.android.libraries.appdoctor.AppDoctorReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.INTERNAL_BROADCAST [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.
27	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.internal.debug.TestingToolsBroadcastReceiver) 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.
28	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.blockstatechanged.BlockStateChangedReceiver) 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.
29	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.accountchanged.AccountChangedReceiver) 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.
30	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.localechanged.LocaleChangedReceiver) 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
31	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.push.PushReceiver) 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.
32	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.restart.RestartReceiver) 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.
33	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.timezonechanged.TimezoneChangedReceiver) 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.
34	Broadcast Receiver (com.google.android.libraries.notifications.platform.entrypoints.update.UpdateReceiver) 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.
35	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.AccountRemovedBroadcastReceiver) 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
36	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeUpdateBackgroundBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [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.
37	Activity (com.google.android.libraries.social.licenses.LicenseMenuActivity) 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.
38	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
39	Activity (androidx.activity.ComponentActivity) 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.
40	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
41	Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [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.
42	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
43	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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	defpackage/aeid.java defpackage/aeif.java defpackage/aeih.java defpackage/aeij.java defpackage/agge.java defpackage/air.java defpackage/akdk.java defpackage/fed.java defpackage/fee.java defpackage/fft.java defpackage/fga.java defpackage/fqx.java defpackage/gsy.java defpackage/vac.java defpackage/wlo.java defpackage/wls.java defpackage/wmd.java defpackage/wne.java defpackage/wre.java defpackage/xjj.java
2	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	defpackage/adej.java defpackage/fnn.java
				defpackage/adkp.java defpackage/adlw.java defpackage/admi.java defpackage/adml.java defpackage/admp.java defpackage/aefb.java defpackage/afbw.java defpackage/afis.java defpackage/afjc.java defpackage/afnm.java defpackage/afnp.java defpackage/afnu.java defpackage/afnv.java defpackage/ahik.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	defpackage/ahnq.java defpackage/aicp.java defpackage/aicq.java defpackage/aimu.java defpackage/ainv.java defpackage/ajgl.java defpackage/ajjt.java defpackage/ajp.java defpackage/awrp.java defpackage/ayoq.java defpackage/ayot.java defpackage/ayov.java defpackage/aysd.java defpackage/aysi.java defpackage/ayth.java defpackage/ayvi.java defpackage/ayxx.java defpackage/azew.java defpackage/azex.java defpackage/azey.java defpackage/azfc.java defpackage/fgi.java defpackage/fhz.java defpackage/fie.java defpackage/fkd.java defpackage/guz.java defpackage/iin.java defpackage/iiq.java defpackage/kpr.java defpackage/kra.java defpackage/krb.java defpackage/lby.java defpackage/pjd.java defpackage/urr.java defpackage/uzb.java defpackage/vac.java defpackage/vng.java defpackage/vnp.java defpackage/woh.java defpackage/wri.java defpackage/xjb.java defpackage/xoq.java defpackage/xow.java defpackage/xoz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j$/util/concurrent/ThreadLocalRandom.java nl/Weave/DeviceManager/WeaveDeviceManager.java
				defpackage/aai.java defpackage/aaxk.java defpackage/abbr.java defpackage/abur.java defpackage/accn.java defpackage/accp.java defpackage/acri.java defpackage/adbx.java defpackage/addr.java defpackage/adji.java defpackage/adlu.java defpackage/adlv.java defpackage/adnv.java defpackage/adok.java defpackage/aelw.java defpackage/aewn.java defpackage/aewu.java defpackage/aexo.java defpackage/af.java defpackage/afeq.java defpackage/afev.java defpackage/affd.java defpackage/afis.java defpackage/afmg.java defpackage/afpa.java defpackage/afpg.java defpackage/afph.java defpackage/afpo.java defpackage/afpp.java defpackage/afpq.java defpackage/afps.java defpackage/afpt.java defpackage/afpv.java defpackage/afpx.java defpackage/afra.java defpackage/afrc.java defpackage/afrh.java defpackage/afrj.java defpackage/afta.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/afxn.java defpackage/agar.java defpackage/agcf.java defpackage/aghh.java defpackage/aghj.java defpackage/aghn.java defpackage/aghs.java defpackage/aght.java defpackage/aghv.java defpackage/aghy.java defpackage/agid.java defpackage/agie.java defpackage/agil.java defpackage/agim.java defpackage/agja.java defpackage/agjd.java defpackage/agjg.java defpackage/agjp.java defpackage/agjx.java defpackage/aglw.java defpackage/agoj.java defpackage/agp.java defpackage/agpx.java defpackage/agtq.java defpackage/agva.java defpackage/agya.java defpackage/agza.java defpackage/agzc.java defpackage/agzo.java defpackage/ahdr.java defpackage/ahfi.java defpackage/ahfj.java defpackage/ahgu.java defpackage/ahgw.java defpackage/ahih.java defpackage/ahil.java defpackage/aib.java defpackage/aimo.java defpackage/aipo.java defpackage/aipx.java defpackage/aiqb.java defpackage/airh.java defpackage/aiwr.java defpackage/aizz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ajcm.java defpackage/ajhc.java defpackage/ajic.java defpackage/ajjt.java defpackage/ajju.java defpackage/ajjz.java defpackage/ajkn.java defpackage/ajkq.java defpackage/ajkw.java defpackage/ajlb.java defpackage/ajlf.java defpackage/ajlg.java defpackage/ajlh.java defpackage/ajlk.java defpackage/ajln.java defpackage/ajlo.java defpackage/ajlp.java defpackage/ajlt.java defpackage/ajlu.java defpackage/ajlw.java defpackage/ajmb.java defpackage/ajnf.java defpackage/ajoq.java defpackage/ajpg.java defpackage/aju.java defpackage/ajvk.java defpackage/ajvp.java defpackage/ajvq.java defpackage/akdk.java defpackage/auaw.java defpackage/aumk.java defpackage/auri.java defpackage/aust.java defpackage/ausv.java defpackage/auth.java defpackage/aw.java defpackage/awtq.java defpackage/aysy.java defpackage/babm.java defpackage/baqx.java defpackage/barc.java defpackage/baro.java defpackage/basf.java defpackage/bkr.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ceh.java defpackage/cl.java defpackage/cnf.java defpackage/ct.java defpackage/da.java defpackage/dbn.java defpackage/dbt.java defpackage/der.java defpackage/dhi.java defpackage/dly.java defpackage/dnv.java defpackage/doh.java defpackage/dqn.java defpackage/drq.java defpackage/drt.java defpackage/drv.java defpackage/dse.java defpackage/dsm.java defpackage/dsw.java defpackage/dsx.java defpackage/dta.java defpackage/dte.java defpackage/dtn.java defpackage/dtq.java defpackage/duc.java defpackage/duh.java defpackage/duk.java defpackage/dul.java defpackage/dun.java defpackage/duq.java defpackage/dvj.java defpackage/dvo.java defpackage/dwd.java defpackage/dwe.java defpackage/dxw.java defpackage/dy.java defpackage/dyd.java defpackage/dzb.java defpackage/eaf.java defpackage/eag.java defpackage/eic.java defpackage/eie.java defpackage/ej.java defpackage/eku.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	defpackage/ekx.java defpackage/elg.java defpackage/elx.java defpackage/emt.java defpackage/emv.java defpackage/en.java defpackage/eq.java defpackage/eyu.java defpackage/ez.java defpackage/ezc.java defpackage/fcw.java defpackage/fu.java defpackage/fwr.java defpackage/fxd.java defpackage/fxm.java defpackage/gev.java defpackage/gho.java defpackage/ghr.java defpackage/ghy.java defpackage/gid.java defpackage/gin.java defpackage/gip.java defpackage/giq.java defpackage/giu.java defpackage/giv.java defpackage/gj.java defpackage/gka.java defpackage/gkd.java defpackage/gkf.java defpackage/gkj.java defpackage/glg.java defpackage/goh.java defpackage/gol.java defpackage/goo.java defpackage/gop.java defpackage/gpn.java defpackage/gsq.java defpackage/gtb.java defpackage/gtg.java defpackage/gwd.java defpackage/gze.java defpackage/gzs.java defpackage/hat.java defpackage/hau.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/hbi.java defpackage/hbr.java defpackage/hbt.java defpackage/hcr.java defpackage/hct.java defpackage/hdc.java defpackage/hdg.java defpackage/hdh.java defpackage/hdj.java defpackage/hed.java defpackage/hef.java defpackage/hen.java defpackage/heo.java defpackage/hft.java defpackage/hgv.java defpackage/hgw.java defpackage/hmm.java defpackage/hnz.java defpackage/hpi.java defpackage/hqc.java defpackage/hqf.java defpackage/hqs.java defpackage/hrz.java defpackage/hw.java defpackage/hwi.java defpackage/hwr.java defpackage/hx.java defpackage/hxn.java defpackage/hzz.java defpackage/iag.java defpackage/iaq.java defpackage/ibj.java defpackage/ibn.java defpackage/ibq.java defpackage/icq.java defpackage/idf.java defpackage/ip.java defpackage/iuk.java defpackage/iul.java defpackage/jk.java defpackage/jte.java defpackage/kcx.java defpackage/kic.java defpackage/kq.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/lae.java defpackage/lai.java defpackage/lj.java defpackage/ls.java defpackage/lsl.java defpackage/lvk.java defpackage/mt.java defpackage/nox.java defpackage/np.java defpackage/oa.java defpackage/oc.java defpackage/og.java defpackage/pb.java defpackage/rjd.java defpackage/rp.java defpackage/sy.java defpackage/ukk.java defpackage/urw.java defpackage/utv.java defpackage/vac.java defpackage/vea.java defpackage/vgw.java defpackage/vkk.java defpackage/vnp.java defpackage/vor.java defpackage/vow.java defpackage/vox.java defpackage/vps.java defpackage/vpt.java defpackage/vqa.java defpackage/vqb.java defpackage/vqc.java defpackage/vqh.java defpackage/vqj.java defpackage/vqk.java defpackage/vqo.java defpackage/vqp.java defpackage/vra.java defpackage/vre.java defpackage/vrf.java defpackage/vrq.java defpackage/vsf.java defpackage/vsm.java defpackage/vsu.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/vsz.java defpackage/vtg.java defpackage/vtm.java defpackage/vtq.java defpackage/vtt.java defpackage/vty.java defpackage/vuc.java defpackage/vuf.java defpackage/vvq.java defpackage/vvv.java defpackage/vvx.java defpackage/vwa.java defpackage/vwd.java defpackage/vwi.java defpackage/vwl.java defpackage/vwp.java defpackage/vwr.java defpackage/vxx.java defpackage/vyh.java defpackage/vyj.java defpackage/vyu.java defpackage/vzd.java defpackage/vzs.java defpackage/vzt.java defpackage/wab.java defpackage/wai.java defpackage/wak.java defpackage/wam.java defpackage/wao.java defpackage/waq.java defpackage/war.java defpackage/wcv.java defpackage/wda.java defpackage/wgb.java defpackage/wgz.java defpackage/whs.java defpackage/wic.java defpackage/wju.java defpackage/wki.java defpackage/wle.java defpackage/wnl.java defpackage/wre.java defpackage/wti.java defpackage/wtw.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/wvc.java defpackage/wvx.java defpackage/wwi.java defpackage/wwq.java defpackage/www.java defpackage/wxo.java defpackage/wxs.java defpackage/wzf.java defpackage/wzh.java defpackage/wzk.java defpackage/wzs.java defpackage/wzw.java defpackage/xab.java defpackage/xbu.java defpackage/xdn.java defpackage/xdx.java defpackage/xiu.java defpackage/xjb.java defpackage/xjc.java defpackage/xjf.java defpackage/xjg.java defpackage/xjj.java defpackage/xjl.java defpackage/xka.java defpackage/xkb.java defpackage/xkf.java defpackage/xki.java defpackage/xko.java defpackage/xkp.java defpackage/xli.java defpackage/xly.java defpackage/xnv.java defpackage/xnw.java defpackage/xob.java defpackage/xwu.java defpackage/yht.java defpackage/yhx.java defpackage/zmk.java defpackage/zpp.java defpackage/zw.java nl/Weave/DataManagement/WdmClientImpl.java
				nl/Weave/DeviceManager/WeaveDeviceManager.java defpackage/aafh.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	defpackage/abno.java defpackage/abpm.java defpackage/abpv.java defpackage/abpw.java defpackage/abqp.java defpackage/aeec.java defpackage/aeed.java defpackage/aeef.java defpackage/aefl.java defpackage/aeko.java defpackage/aely.java defpackage/aend.java defpackage/aetu.java defpackage/afks.java defpackage/afrq.java defpackage/agco.java defpackage/ahfy.java defpackage/ahfz.java defpackage/ajzo.java defpackage/akan.java defpackage/amjp.java defpackage/amjt.java defpackage/amks.java defpackage/amnr.java defpackage/amok.java defpackage/ampt.java defpackage/anwp.java defpackage/anxh.java defpackage/aqcc.java defpackage/aqdl.java defpackage/armg.java defpackage/ayud.java defpackage/bnq.java defpackage/bsd.java defpackage/cdm.java defpackage/cen.java defpackage/fdm.java defpackage/hex.java defpackage/hti.java defpackage/hut.java defpackage/hvn.java defpackage/hvv.java defpackage/ntr.java defpackage/nvi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/nwv.java defpackage/nxm.java defpackage/nxu.java defpackage/nyv.java defpackage/pzr.java defpackage/sns.java defpackage/uao.java defpackage/ulu.java defpackage/yon.java
6	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	defpackage/yyf.java defpackage/afis.java defpackage/ajnf.java defpackage/rvw.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	defpackage/aaqv.java defpackage/aaqx.java defpackage/abff.java defpackage/adyu.java defpackage/aedn.java defpackage/ahii.java defpackage/axsx.java defpackage/badr.java defpackage/badx.java defpackage/bady.java defpackage/bael.java defpackage/bafb.java defpackage/bafc.java defpackage/bafd.java defpackage/bafe.java defpackage/bagm.java defpackage/bahf.java defpackage/bahi.java defpackage/lci.java defpackage/qzb.java defpackage/rdc.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	defpackage/pos.java defpackage/tzj.java defpackage/xli.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	defpackage/abzf.java defpackage/ahfi.java defpackage/xap.java
10	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	defpackage/adej.java defpackage/adxe.java defpackage/agar.java defpackage/agid.java defpackage/agsc.java defpackage/ahfq.java defpackage/ajdk.java defpackage/ajjt.java defpackage/ajkn.java defpackage/ajlf.java defpackage/awtr.java defpackage/iio.java defpackage/vxy.java
11	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	defpackage/aggy.java defpackage/ajfx.java defpackage/basc.java defpackage/wri.java defpackage/xoz.java
12	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	defpackage/agcn.java defpackage/dtr.java defpackage/xjl.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/actk.java defpackage/afph.java defpackage/aheq.java
14	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	defpackage/ili.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	defpackage/advh.java defpackage/adxj.java defpackage/afbw.java defpackage/afjt.java defpackage/afmm.java defpackage/afph.java defpackage/agcr.java defpackage/agdh.java defpackage/aitd.java defpackage/ajnf.java defpackage/aw.java defpackage/awhq.java defpackage/azza.java defpackage/baqj.java defpackage/baqz.java defpackage/basf.java defpackage/dte.java defpackage/duk.java defpackage/dul.java defpackage/ecb.java defpackage/eie.java defpackage/fej.java defpackage/ffh.java defpackage/fgh.java defpackage/hig.java defpackage/hrb.java defpackage/hta.java defpackage/htb.java defpackage/hxr.java defpackage/lra.java defpackage/tcq.java defpackage/wss.java defpackage/xnb.java j$/desugar/sun/nio/fs/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	defpackage/aerk.java defpackage/afis.java defpackage/afkw.java defpackage/aftq.java defpackage/agcn.java defpackage/agcr.java defpackage/awhq.java defpackage/dme.java defpackage/ecd.java defpackage/ece.java defpackage/ech.java defpackage/gqn.java defpackage/hig.java defpackage/hmn.java defpackage/xjk.java defpackage/xwe.java
00024	Write file after Base64 decoding	reflection file	defpackage/afis.java defpackage/hig.java
			defpackage/abgb.java defpackage/abtn.java defpackage/acnh.java defpackage/adaw.java defpackage/adej.java defpackage/aeiz.java defpackage/aejf.java defpackage/aewu.java defpackage/agkh.java defpackage/avg.java defpackage/baxe.java defpackage/dot.java defpackage/frf.java defpackage/gix.java defpackage/hcl.java defpackage/hqg.java defpackage/hrs.java defpackage/iku.java defpackage/ilb.java defpackage/ili.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	defpackage/ilm.java defpackage/imu.java defpackage/iot.java defpackage/isa.java defpackage/iwr.java defpackage/ixi.java defpackage/jbh.java defpackage/jfz.java defpackage/jme.java defpackage/jyz.java defpackage/kbd.java defpackage/kiz.java defpackage/kpx.java defpackage/kwb.java defpackage/kwi.java defpackage/kxn.java defpackage/lct.java defpackage/ldk.java defpackage/lhs.java defpackage/liu.java defpackage/lmg.java defpackage/lmt.java defpackage/lue.java defpackage/lvk.java defpackage/lvq.java defpackage/lwt.java defpackage/lxv.java defpackage/lyb.java defpackage/msh.java defpackage/myj.java defpackage/nas.java defpackage/nax.java defpackage/ndr.java defpackage/npb.java defpackage/oan.java defpackage/ofa.java defpackage/oju.java defpackage/onc.java defpackage/osh.java defpackage/otf.java defpackage/pam.java defpackage/pbl.java defpackage/pbx.java defpackage/pck.java

RULE ID	BEHAVIOUR	LABEL	FILES
			defpackage/pcl.java defpackage/pdb.java defpackage/pde.java defpackage/pfq.java defpackage/pjk.java defpackage/pnn.java defpackage/pny.java defpackage/poa.java defpackage/pry.java defpackage/psj.java defpackage/qhs.java defpackage/qjd.java defpackage/qjp.java defpackage/qmi.java defpackage/qtz.java defpackage/qug.java defpackage/quw.java defpackage/qym.java defpackage/rbn.java defpackage/rcv.java defpackage/riw.java defpackage/rvw.java defpackage/sep.java defpackage/spe.java defpackage/stj.java defpackage/szc.java defpackage/tcs.java defpackage/tdb.java defpackage/tes.java defpackage/tfa.java defpackage/tfc.java defpackage/tzj.java defpackage/udd.java defpackage/vac.java defpackage/vqa.java defpackage/vqq.java defpackage/wff.java defpackage/wpm.java defpackage/wpo.java defpackage/wre.java defpackage/xbm.java defpackage/xbt.java defpackage/xbu.java defpackage/xcg.java

RULE ID	BEHAVIOUR	LABEL	FILES
			defpackage/xjn.java defpackage/xkp.java defpackage/xli.java defpackage/xoc.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	defpackage/abtn.java defpackage/adaw.java defpackage/aeiz.java defpackage/aejf.java defpackage/baxe.java defpackage/dot.java defpackage/hrs.java defpackage/ilm.java defpackage/jme.java defpackage/kiz.java defpackage/kwi.java defpackage/kxn.java defpackage/lue.java defpackage/lvk.java defpackage/lxv.java defpackage/lyb.java defpackage/myj.java defpackage/npb.java defpackage/ofa.java defpackage/oju.java defpackage/osh.java defpackage/otf.java defpackage/pjk.java defpackage/qtz.java defpackage/qug.java defpackage/qym.java defpackage/rcv.java defpackage/sep.java defpackage/tcs.java defpackage/tdb.java defpackage/tzj.java defpackage/udd.java defpackage/vqq.java defpackage/xbm.java defpackage/xbu.java defpackage/xjn.java

RULE ID	BEHAVIOUR	LABEL	FILES
00023	Start another application from current application	reflection control	defpackage/lvk.java defpackage/pry.java defpackage/qas.java defpackage/tcs.java
00112	Get the date of the calendar event	collection calendar	defpackage/rtl.java defpackage/uwr.java
00036	Get resource file from res/raw directory	reflection	defpackage/abgb.java defpackage/afpj.java defpackage/afsz.java defpackage/afta.java defpackage/agbt.java defpackage/agid.java defpackage/ffh.java defpackage/hqg.java defpackage/hrs.java defpackage/hxn.java defpackage/iio.java defpackage/jxh.java defpackage/lai.java defpackage/lvk.java defpackage/lxv.java defpackage/nas.java defpackage/npb.java defpackage/oan.java defpackage/ofa.java defpackage/pjk.java defpackage/tdb.java defpackage/vac.java defpackage/vqq.java defpackage/vtg.java defpackage/xiv.java defpackage/xwu.java
00130	Get the current WIFI information	wifi collection	defpackage/abss.java defpackage/absw.java defpackage/tfx.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	defpackage/ajkq.java defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/kcx.java defpackage/xap.java defpackage/yjd.java defpackage/zcg.java
00089	Connect to a URL and receive input stream from the server	command network	defpackage/ajkq.java defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/hub.java defpackage/yjd.java defpackage/zcg.java
00030	Connect to the remote server through the given URL	network	defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/hub.java defpackage/wnp.java defpackage/wps.java defpackage/yjd.java
00109	Connect to a URL and get the response code	network command	defpackage/ajkq.java defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/hub.java defpackage/vac.java defpackage/vfe.java defpackage/wnp.java defpackage/wps.java defpackage/xap.java defpackage/yjd.java
00034	Query the current data network type	collection network	defpackage/xkp.java

RULE ID	BEHAVIOUR	LABEL	FILES
00139	Get the current WiFi id	collection wifi	defpackage/absw.java
00134	Get the current WiFi IP address	wifi collection	defpackage/absw.java
00075	Get location of the device	collection location	defpackage/ajp.java
00137	Get last known location of the device	location collection	defpackage/ajp.java
00079	Hide the current app's icon	evasion	defpackage/hha.java defpackage/xjh.java
00091	Retrieve data from broadcast	collection	defpackage/aeeh.java defpackage/ajic.java defpackage/ajlb.java defpackage/brk.java defpackage/hdc.java defpackage/nlr.java defpackage/oos.java defpackage/oty.java defpackage/pjr.java defpackage/vqa.java defpackage/wpo.java
00012	Read data and put it into a buffer stream	file	defpackage/awhq.java defpackage/eie.java defpackage/fgh.java
00094	Connect to a URL and read data from it	command network	defpackage/aiaw.java defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/xap.java
00108	Read the input stream from given URL	network command	defpackage/bare.java defpackage/fev.java defpackage/hig.java defpackage/zll.java

RULE ID	BEHAVIOUR	LABEL	FILES
00058	Connect to the specific WIFI network	wifi control	defpackage/abtd.java
00153	Send binary data over HTTP	http	defpackage/hot.java
00202	Make a phone call	control	defpackage/kiz.java defpackage/kwi.java
00203	Put a phone number into an intent	control	defpackage/kiz.java defpackage/kwi.java
00014	Read file into a stream and put it into a JSON object	file	defpackage/ajnf.java defpackage/basf.java
00123	Save the response to JSON after connecting to the remote server	network command	defpackage/xan.java defpackage/xar.java defpackage/yjd.java
00128	Query user account information	collection account	defpackage/adoe.java defpackage/adof.java defpackage/zll.java
00009	Put data in cursor to JSON object	file	defpackage/xjt.java
00028	Read file from assets directory	file	defpackage/feg.java
00162	Create InetSocketAddress object and connecting to it	socket	defpackage/awtn.java defpackage/awtq.java
00163	Create new Socket and connecting to it	socket	defpackage/awtn.java defpackage/awtq.java
00015	Put buffer stream (data) to JSON object	file	defpackage/xap.java
00056	Modify voice volume	control	org/webrtc/audio/WebRtcAudioTrack.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory	file command	defpackage/auaw.java
00004	Get filename and put it to JSON object	file collection	defpackage/auaw.java
00125	Check if the given file path exist	file	defpackage/ajmb.java defpackage/auaw.java
00104	Check if the given path is directory	file	defpackage/auaw.java
00132	Query The ISO country code	telephony collection	defpackage/fvo.java
00102	Set the phone speaker on	command	defpackage/yia.java
00187	Query a URI and check the result	collection sms calllog calendar	defpackage/afpa.java
00072	Write HTTP input stream into a file	command network file	defpackage/hig.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://com-api-project-498579633514.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/498579633514/namespaces/firebase:fetch?key=AIzaSyD4Ok1UA0HHmyKCm5s_cQhWD7ZHZwnhorc. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	9/44	android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.CALL_PHONE, android.permission.ACCESS_BACKGROUND_LOCATION

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 104.18.27.120 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
myaccount-staging.corp.google.com	ok	**IP:** 74.125.138.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
staging-notifications-pa.sandbox.googleapis.com	ok	**IP:** 74.125.196.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.98.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
onhub.here	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 192.178.50.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 192.178.50.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
crash.corp.google.com	ok	**IP:** 74.125.138.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
one.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
notifications-pa.googleapis.com	ok	**IP:** 142.250.217.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
policies.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
g.co	ok	**IP:** 142.251.34.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh6.googleusercontent.com	ok	**IP:** 172.217.3.65 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.facebook.com	ok	**IP:** 57.144.22.1 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
staging-qual-qa-notifications-pa.sandbox.googleapis.com	ok	**IP:** 172.217.204.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
home.ft.nest.com	ok	**IP:** 34.96.80.13 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developers.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
csp.withgoogle.com	ok	**IP:** 142.250.217.209 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
autopush-qual-playground-notifications-pa.sandbox.googleapis.com	ok	**IP:** 173.194.216.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
clients5.google.com	ok	**IP:** 172.217.2.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
com.google.android.apps.chromecast.app	ok	No Geolocation information available.
nest.com	ok	**IP:** 35.241.20.76 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dev-notifications-pa.corp.googleapis.com	ok	**IP:** 74.125.136.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
maps.googleapis.com	ok	**IP:** 142.250.64.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.64.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
assistant.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
encrypted-tbn0.gstatic.com	ok	**IP:** 142.250.64.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
home.nest.com	ok	**IP:** 34.117.101.60 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
nestservices.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
clients.nest.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
myaccount.google.com	ok	**IP:** 172.217.203.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
autopush-notifications-pa.sandbox.googleapis.com	ok	**IP:** 74.125.134.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nestauthproxyservice-pa.googleapis.com	ok	**IP:** 172.217.2.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
storage.googleapis.com	ok	**IP:** 172.217.165.219 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
cast.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 192.178.50.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.class.d.getcls	ok	No Geolocation information available.
madeby.google.com	ok	**IP:** 142.251.35.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
encrypted-tbn3.gstatic.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pay.google.com	ok	**IP:** 172.217.204.92 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 142.250.64.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
oauthintegrations.googleapis.com	ok	**IP:** 142.251.35.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.64.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
encrypted-tbn2.gstatic.com	ok	**IP:** 142.251.35.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
takeout.google.com	ok	**IP:** 172.217.15.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
encrypted-tbn1.gstatic.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
partnerdash.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh3.googleusercontent.com	ok	**IP:** 192.178.50.33 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh4.googleusercontent.com	ok	**IP:** 192.178.50.33 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clients3.google.com	ok	**IP:** 192.178.50.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nest.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
families.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
home.qa.nestlabs.com	ok	**IP:** 54.156.88.210 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
android.googleapis.com	ok	**IP:** 216.239.38.223 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
store.google.com	ok	**IP:** 172.217.3.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play-lh.googleusercontent.com	ok	**IP:** 142.250.217.182 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
com-api-project-498579633514.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
nest-open-source.googlesource.com	ok	**IP:** 74.125.134.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.251.34.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 172.217.15.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.64.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
preview.home.google.com	ok	**IP:** 142.251.34.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.nest.com	ok	**IP:** 35.241.20.76 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
webapi.camera.home.nest.com	ok	**IP:** 35.201.70.64 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
myactivity.google.com	ok	**IP:** 142.250.98.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nestrenew.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dogfood.home.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
myadcenter.google.com	ok	**IP:** 142.250.64.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.class.e.getcls	ok	No Geolocation information available.
www.gstatic.com	ok	**IP:** 192.178.50.35 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.13.145 **Country:** United States of America **Region:** Florida **City:** Miami **Latitude:** 25.774269 **Longitude:** -80.193657 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
lh5.googleusercontent.com	ok	**IP:** 142.251.35.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
home.google.com	ok	**IP:** 192.178.50.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
eureka-df-triage@google.com	defpackage/lxi.java
u0013android@android.com0 u0013android@android.com	defpackage/vqw.java
id-tv-remote-support@google.com	defpackage/baen.java

TRACKERS

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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://com-api-project-498579633514.firebaseio.com"
"google_api_key" : "AIzaSyD4Ok1UA0HHmyKCm5s_cQhWD7ZHZwnhorc"
"google_crash_reporting_api_key" : "AIzaSyD4Ok1UA0HHmyKCm5s_cQhWD7ZHZwnhorc"
"two_factor_auth_button_cancel" : "Cancel"
"two_factor_auth_button_ok" : "OK"
"view_wifi_credentials_network_password" : "Password"
"wan_settings_pppoe_password" : "Password"
E5B59E5A-774F-49D7-9DE0-7504B099EC50
3C77AC08-464F-49D2-BC3C-EF2BAA36DB22
2d8fd5c6-f991-496c-aa05-6a5e3953a1af
9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
0b6aa300-0576-11e5-b9a5-0002a5d5c51b
246C6160-FAB2-11E4-9FBB-0002A5D5C51B
256C6160-FAB2-11E4-9FBB-0002A5D5C51B
0728fe40-002f-11e5-87d0-0002a5d5c51b
5B20CF8B-0D01-4C32-BF6B-F4FC9FF1DEA0
007c6160-fab2-11e4-9fbb-0002a5d5c51b
0028fe40-002f-11e5-87d0-0002a5d5c51b
297C6160-FAB2-11E4-9FBB-0002A5D5C51B
0fde7f14-864a-4f7f-8dbe-7ac1f4ea4b91
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
046aa300-0576-11e5-b9a5-0002a5d5c51b
176c6160-fab2-11e4-9fbb-0002a5d5c51b
7606123e-4282-4ed4-aca1-2374de7fdb61

POSSIBLE SECRETS
cfcb3523-8ce7-43d8-9670-a0456b2dd71c
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
FF5ECE48-D50B-42B9-937A-6E5918A9426C
0528fe40-002f-11e5-87d0-0002a5d5c51b
CgJhdAoCYmUKAmJnCgJjeQoCY3oKAmRlCgJkawoCZWUKAmVzCgJmaQoCZnIKAmdyCgJodQoCaHIKAmllCgJpdAoCbHYKAmx0CgJsdQoCbXQKAm5sCgJwbAoCcHQKAnJvCgJzaQoCc2UKAnNr
167C6160-FAB2-11E4-9FBB-0002A5D5C51B
CilhY3Rpb24uZGV2aWNlcy50eXBlcy5BVURJT19WSURFT19SRUNFSVZFUgocYWN0aW9uLmRldmljZXMudHlwZXMuQkFUVEVSWQoYYWN0aW9uLmRldmljZXMudHlwZXMuQkVEChxhY3Rpb24uZGV2aWNlcy50eXBlcy5CTEVOREVSChthY3Rpb24uZGV2aWNlcy50eXBlcy5DQU1FUkEKHGFjdGlvbi5kZXZpY2VzLnR5cGVzLkNIQVJHRVIKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLkRJU0hXQVNIRVIKGmFjdGlvbi5kZXZpY2VzLnR5cGVzLkRSWUVSChxhY3Rpb24uZGV2aWNlcy50eXBlcy5ESVNQTEFZChlhY3Rpb24uZGV2aWNlcy50eXBlcy5ET09SCh1hY3Rpb24uZGV2aWNlcy50eXBlcy5ET09SQkVMTAobYWN0aW9uLmRldmljZXMudHlwZXMuRFJBV0VSChthY3Rpb24uZGV2aWNlcy50eXBlcy5GQVVDRVQKHmFjdGlvbi5kZXZpY2VzLnR5cGVzLkZJUkVQTEFDRQocYWN0aW9uLmRldmljZXMudHlwZXMuRlJFRVpFUgoaYWN0aW9uLmRldmljZXMudHlwZXMuRlJZRVIKIWFjdGlvbi5kZXZpY2VzLnR5cGVzLkdBTUVfQ09OU09MRQobYWN0aW9uLmRldmljZXMudHlwZXMuR0FSREVOCiBhY3Rpb24uZGV2aWNlcy50eXBlcy5HT09HTEVfSE9NRQoaYWN0aW9uLmRldmljZXMudHlwZXMuR1JJTEwKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLkhFQURQSE9ORVMKGWFjdGlvbi5kZXZpY2VzLnR5cGVzLktFVFRMRQoeYWN0aW9uLmRldmljZXMudHlwZXMuTUlDUk9XQVZFCiBhY3Rpb24uZGV2aWNlcy50eXBlcy5NVUxUSUNPT0tFUgocYWN0aW9uLmRldmljZXMudHlwZXMuTkVUV09SSwoZYWN0aW9uLmRldmljZXMudHlwZXMuT1ZFTgoeYWN0aW9uLmRldmljZXMudHlwZXMuUEVURkVFREVSCiNhY3Rpb24uZGV2aWNlcy50eXBlcy5QUkVTU1VSRUNPT0tFUgohYWN0aW9uLmRldmljZXMudHlwZXMuUkVGUklHRVJBVE9SCiJhY3Rpb24uZGV2aWNlcy50eXBlcy5SRU1PVEVDT05UUk9MChlhY3Rpb24uZGV2aWNlcy50eXBlcy5ST09GChthY3Rpb24uZGV2aWNlcy50eXBlcy5ST1VURVIKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLlNNT0tFX0RFVEVDVE9SCh1hY3Rpb24uZGV2aWNlcy50eXBlcy5TT1VTVklERQocYWN0aW9uLmRldmljZXMudHlwZXMuU1BFQUtFUgoiYWN0aW9uLmRldmljZXMudHlwZXMuU1BFQUtFUl9HUk9VUAohYWN0aW9uLmRldmljZXMudHlwZXMuU1BFQUtFUl9QQUlSCh5hY3Rpb24uZGV2aWNlcy50eXBlcy5TUFJJTktMRVIKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLlNUQU5ETUlkVBTUlOR19CT1gKJ2FjdGlvbi5kZXZpY2VzLnR5cGVzLlNUUkVBTUlOR19CT1gKImFjdGlvbi5kZXZpY2VzLnR5cGVzLlNUUkVBTUlOR19TT1VOREJBUgokYWN0aW9uLmRldmljZXMudHlwZXMuU1RSUFNSU5HX1NUSUNLCh9hY3Rpb24uZGV2aWNlcy50eXBlcy5TUEVSTU9TVEFUChthY3Rpb24uZGV2aWNlcy50eXBlcy5TUT0lMRVQKGmFjdGlvbi5kZXZpY2VzLnR5cGVzLlZBTFZFCh9hY3Rpb24uZGV2aWNlcy50eXBlcy5WRU5USUxBVE9SChthY3Rpb24uZGV2aWNlcy50eXBlcy5XQVRFUlBVUklGSUVSCiJhY3Rpb24uZGV2aWNlcy50eXBlcy5XQVRFUlNPRlRFTkVSCiNhY3Rpb24uZGV2aWNlcy50eXBlcy5XRUFUSEVSU1RBVElPTgofYWN0aW9uLmRldmljZXMudHlwZXMuV0lORUNFTExBUgogYWN0aW9uLmRldmljZXMudHlwZXMuWU9HVVJUTUFLRVI
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
277C6160-FAB2-11E4-9FBB-0002A5D5C51B

POSSIBLE SECRETS
086aa300-0576-11e5-b9a5-0002a5d5c51b
067c6160-fab2-11e4-9fbb-0002a5d5c51b
167c6160-fab2-11e4-9fbb-0002a5d5c51b
7452D29F-5B88-4709-8776-6F4509D543B5
F1CACD13-1FED-4A9D-87B7-FB4CFC526F3B
0328fe40-002f-11e5-87d0-0002a5d5c51b
227C6160-FAB2-11E4-9FBB-0002A5D5C51B
6fa872e89ed53f1f00ecd64797f62115
ea4ce6093b9d29b56181718d906e0024
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
1a6c6160-fab2-11e4-9fbb-0002a5d5c51b
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
BC596295-EB44-424E-9EE8-D3510863420A
087c6160-fab2-11e4-9fbb-0002a5d5c51b

POSSIBLE SECRETS
70012FC8-1A6E-4FA1-B300-552528906093
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
6DC0EC50-8B6A-4E47-BCF6-2C6495D6499B
1c7c6160-fab2-11e4-9fbb-0002a5d5c51b
8P1sW0EPJcslw7UzRsiXL64w+O50Ed+RBICtay1g24M=
ebfb9f16-d6e5-421f-a53d-c57bf2ed703f
ChNmcm9udGVuZC90aHVtYm5haWxzCiFkb3dubG9hZC90aHVtYm5haWxzL2V2ZW50LXByZXZpZXc
85cc9b331002775d21add9c2665e440c
8d5155894229d5e689ee01e6018a237e2cae64cd
287C6160-FAB2-11E4-9FBB-0002A5D5C51B
1a7c6160-fab2-11e4-9fbb-0002a5d5c51b
197c6160-fab2-11e4-9fbb-0002a5d5c51b
0428fe40-002f-11e5-87d0-0002a5d5c51b
1E7C6160-FAB2-11E4-9FBB-0002A5D5C51B
0A68DA69-C87A-4461-A68D-FB0DAE115060
027c6160-fab2-11e4-9fbb-0002a5d5c51b
166c6160-fab2-11e4-9fbb-0002a5d5c51b

POSSIBLE SECRETS
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
047c6160-fab2-11e4-9fbb-0002a5d5c51b
057c6160-fab2-11e4-9fbb-0002a5d5c51b
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
257C6160-FAB2-11E4-9FBB-0002A5D5C51B
1E6C6160-FAB2-11E4-9FBB-0002A5D5C51B
9760508f15230bccb292b982a2eb840bf0581cf5
d2d3f8ef-9c99-4d9c-a2b3-91c85d44326c
A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
c0becc4e166b53571e4145f720e57787
127c6160-fab2-11e4-9fbb-0002a5d5c51b
90e50a2880874523b593ebed2f5df7ed
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

POSSIBLE SECRETS
E64AA4C2-CF37-4FD3-8EC0-D4D6EAC6E09E
7b4a6a59292e18bdb45d33bd6152c7d2
247C6160-FAB2-11E4-9FBB-0002A5D5C51B
Ch9hY3Rpb24uZGV2aWNlcy50eXBlcy5BQ19IRUFUSU5HChxhY3Rpb24uZGV2aWNlcy50eXBlcy5BQ19VTklUCh5hY3Rpb24uZGV2aWNlcy50eXBlcy5BSVJDT09MRVIKIWFjdGlvbi5kZXZpY2VzLnR5cGVzLkFJUkZSRVNIRU5FUgogYWN0aW9uLmRldmljZXMudHlwZXMuQUlSUFVSSUZJRVIKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLkJPSUxFUgohYWN0aW9uLmRldmljZXMudHlwZXMuREVIVU1JRElGSUVSChhhY3Rpb24uZGV2aWNlcy50eXBlcy5GQU4KHmFjdGlvbi5kZXZpY2VzLnR5cGVzLkZJUkVQTEFDRQobYWN0aW9uLmRldmljZXMudHlwZXMuSEVBVEVSChlhY3Rpb24uZGV2aWNlcy50eXBlcy5IT09ECh9hY3Rpb24uZGV2aWNlcy50eXBlcy5IVU1JRElGSUVSCh1hY3Rpb24uZGV2aWNlcy50eXBlcy5SQURJQVRPUgobYWN0aW9uLmRldmljZXMudHlwZXMuU0VOU09SCh9hY3Rpb24uZGV2aWNlcy50eXBlcy5USEVSTU9TVEFU
0228fe40-002f-11e5-87d0-0002a5d5c51b
0128fe40-002f-11e5-87d0-0002a5d5c51b
3ec74551057a2580be0eb5a7c58e96a4
066aa300-0576-11e5-b9a5-0002a5d5c51b
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
bf62dbc920b36c8a13d8e11e933636e9
2DAB7A51-4BC8-4349-9624-46F1411FD030
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1cbd3130fa23b59692c061c594c16cc0
117c6160-fab2-11e4-9fbb-0002a5d5c51b

POSSIBLE SECRETS
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
962eddcc369cba8ebb260ee6b6a126d9346e38c5
0828fe40-002f-11e5-87d0-0002a5d5c51b
115792089210356248762697446949407573530086143415290314195533631308867097853951
ChduZXN0LWhvbWUtYXNzaXN0YW50LWRldgoWbmVzdC1ob21lLWFzc2lzdGFudC1xYQoWbmVzdC1ob21lLWFzc2lzdGFudC1mdAoYbmVzdC1ob21lLWFzc2lzdGFudC1wcm9k
AIzaSyDgmW4ZMvNblSXqMOgsbY8uRrTnfR3E7pY
CihodHRwczpcL1wvZG9nZm9vZFwuaG9tZVwuZ29vZ2xlXC5jb21cLy4qCihodHRwczpcL1wvcHJldmlld1wuaG9tZVwuZ29vZ2xlXC5jb21cLy4qCh9odHRwczpcL1wvaG9tZVwuZ29vZ2xlXC5jb21cLy4q
744020a6-cee3-4e5a-9a6c-b728e9109b0b
CgJlbgoFZGUtREUKBWphLUpQCgVlcy1FUwoFZXMtTVgKBWVzLVVTCgVwdC1CUgoFZnItRlIKBWZyLUNBCgVpdC1JVAoFaGktSU4KBWtvLUtSCgV6aC1UVwoFZXMtQVIKBWVzLUNMCgVlcy1DTwoFZXMtUEUKBW5sLU5MCgVuby1OTwoFbmItTk8KBXN2LVNFCgVkYS1ESwoFYXItRUcKBWFyLVNBCgVpZC1JRAoFcGwtUEwKBWRlLUJFCgVmci1CRQoFbmwtQkUKBWRlLUFUCgVkZS1DSAoFZnItQ0gKBWl0LUNI
CgJhdAoCYXgKAmJlCgJiZwoCY2gKAmN5CgJjegoCZGUKAmRrCgJlZQoCZXMKAmZpCgJmcgoCZ2IKAmdyCgJodQoCaHIKAmllCgJpdAoCbHYKAmx0CgJsdQoCbXQKAm5sCgJwbAoCcHQKAnJvCgJzawoCc2kKAnNl
cbbfe0e2-f7f3-4206-84e0-84cbb3d09dfc

POSSIBLE SECRETS

ChphY3Rpb24uZGV2aWNlcy50eXBlcy5MSUdIVAobYWN0aW9uLmRldmljZXMudHlwZXMuT1VUTEVUChthY3Rpb24uZGV2aWNlcy50eXBlcy5TV0lUQ0gKF2FjdGlvbi5kZXZpY2VzLnR5cGVzLlRWCh9hY3Rpb24uZGV2aWNlcy50eXBlcy5USEVSTU9TVEFUChxhY3Rpb24uZGV2aWNlcy50eXBlcy5TUEVBS0VSChxhY3Rpb24uZGV2aWNlcy50eXBlcy5BQ19VTklUChthY3Rpb24uZGV2aWNlcy50eXBlcy5WQUNVVU0KIWFjdGlvbi5kZXZpY2VzLnR5cGVzLkdBTUVfQ09OU09MRQoYYWN0aW9uLmRldmljZXMudHlwZXMuRkFOCiJhY3Rpb24uZGV2aWNlcy50eXBlcy5TVFJFQU1JTkdfQk9YCiBhY3Rpb24uZGV2aWNlcy50eXBlcy5BSVJQVVJJRklFUgobYWN0aW9uLmRldmljZXMudHlwZXMuU0VUVE9QCiRhY3Rpb24uZGV2aWNlcy50eXBlcy5TVFJFQU1JTkdfU1RJQ0sKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLlkhVTUlESUZJRVIKHGFjdGlvbi5kZXZpY2VzLnR5cGVzLlNZTkNCT1gKKWFjdGlvbi5kZXZpY2VzLnR5cGVzLkxFVRElPX1ZJREVPX1JFQ0VJVkVSChxhY3Rpb24uZGV2aWNlcy50ESVNQTEFZChthY3Rpb24uZGV2aWNlcy50eXBlcy5LRVRUTEUKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLlldBU0hFUgodYWN0aW9uLmRldmljZXMudHlwZXMuU09VTkRCQVIKIWFjdGlvbi5kZXZpY2VzLnR5cGVzLkNPRkZRV9NQUtFUgofYWN0aW9uLmRldmljZXMudHlwZXMuRElTSFdBU0hFUgoaYWN0aW9uLmRldmljZXMudHlwZXMuRFJZRVIKIWFjdGlvbi5kZXZpcY2VzLnR5cGVzLkFJUkZSRVNIRU5FUgohYWN0aW9uLmRldmljZXMudHlwZXMuREVlVU1JRElGSUVSChhhY3Rpb24uZGV2aWNlcy50eXBlcy5NT1AKGWFjdGlvbi5kZXZpcY2VzLnR5cGVzLkhPT0QKJ2FjdGlvbi5kZXZpcY2VzLnR5cGVzLlNUUkVBTUlOR19TT1VOREJBUg

FF0C3832-19B0-447F-B444-9E20CA1254C9

0c7c6160-fab2-11e4-9fbb-0002a5d5c51b

D89CB60A-CFCE-4DE5-A534-B021450B59BA

CiYKEUNvbS5zZW5nbGVkLmxpZmUyEhFzZW5nbGVkcHJvZC03MTYzZAowCh1haWZhLnJlbW90ZWNvbnRyb2wudHcud2lmaS5ocBIPc21hcnRob21lLTZhOWMzCiIKD2FwcC5nb29kbGlmZS5waxIPZ29vZC1saWZlLTc3NjE4CioKCWFwcC5ob21leRIdYXRob20tY2xvdWQtYXNzaXN0YW50LWRldmljZXMKIAoNYXBwLmxhdW5kcmlmeRIPbGF1bmRyaWZ5LTQzZDJmCi8KGmF1LmNvbS5nc21pbm5vdmF0aW1pcmG9sby5uZXQudjMSHGNoaXBvbG8tYXNzaXN0YW50LWRldmljZXMKIAoNYXBwLmxhdW5kcmlmeRIPbGF1bmRyaWZ5LTQzZDJmCiZici5jb20uaW50ZWxpcmFzLnNtYXJ0LWhvbWUKNgoeY24uY29tLmJyb2FkbGluay5lY29udHJvbC5wbHVzEhRicm9hZGxpbmstc21hcnQtNjQzNjIKLgoOY2hpcG9sby5uZXQudjMSHGNoaXBvbG8tYXNzaXN0YW50LWRldmljZXMKIAoQY29tLmFib2RlLmFib2RlEhBhYm9kZS1zbWFydC1ob21lCh8KD2NvbS5hZGRsb24uaG9tZRIMYWRkbG9uLXNtYXJ0CiQKD2NvbS5hZHQucHVsc2USE2FkdC1wdWxzZS1zbWFydGhvbWUKJwoTY29tLmFlZy50eWFlZy50YXN0ZRIQYWVnLWtpdGNoZW4tcHJvZAoaCgxjb20uYWVuby5zZGESCmFlbm8tMTkyZmQKGgoMY29tLmFmdG8uaW90EgphZnRvLTQwNzc0Ch4KDGNvbS5haS5zbWFydBIOYWktc21hcnQtN2NmMjkKJQoSY29tLmFpcmhlYWx0aC5za3llEg9haXItaGVhbHRoLXNreWUKJgoVY29tLmFpc2lyZXluc21hcnRidWxiEg1haXNpcmVyLXNtYXJ0CioKFWNvbS5haXRla2JyYXNpbC5zbWFydBIRYWl0ZWstc21hcnQtYjZkYTgKIQoNY29tLmFsaXN0ZTAwNBIQYWxpc3RlLXNtYXJ0aG9tZQorChRjb20uYWxsZWdpb24ubGVvcHRjb20uYWxsZWdpb24ubGVvcGFyZBITc2NobGFnZS1zZW5zZS0zZDBjMQokCgpjb20uYXAuYm1yEhZiaW1hci1saXZlLXNtYXJ0LWM3NmE5Ch8KEGNvbS5hcGVtYW4ubm9vaWUSC25vb2llLWI2OThlCjUKFWNvbS5hcmxlYy5ncmlkY29ubmVjdBIcZ3JpZGhvbWUtc21hcnRjb250cm9sLWFjdGlvbgomChNjb20uYXNwZW4ud2luZG93ZmFuEg9hc3BlbmhvbWUtOTE5ZDYKKwocY29tLmFzeW5jaHJvbnkuZW1lcnNvbi5zZW5zaRILc2Vuc2ktM2NjYjUKHgoPY29tLmF0b21pLnNtYXJ0EgthdG9taS1zbWFydC5ob21lEg9hdmF0YXItY29udHJvbHMKKgoWY29tLmF6dGVjaC5nbHVzZS1zbWFydC5ob21lEg9hdmF0YXItY29udHJvbHMKKgoWY29tLmF6dG9tZQomChZjb20uYmVsa2luLndlbW9hbmRyb2lkEgx3ZW1vLWNvbnRyb2wKLgoaY29tLmJsaXNzbGlnaHRzLnNtYXJ0Ymxpc3MEHNtYXJ0Ymxpc3MtMWM5MmIKLQoUY29tLmJyZXZpbGxlLmNvbm5lY3QSFWJyZXZpbGxlLWhvbWUtY29ubmVjdAouChtjb20uYnJpbGxpYW50bGlnaHRzLnNtYXJ0Ymxpc3MtMWM5MmIKLQoUY29tLmJyZXZpbGxlLWhvbWUtY29ubmVjdAouChtjb20uYnJpbGxpYW50bGlnaHRpbmcuYnJhaW4SD2JyaWxsaWFudC1zbWFydAo7CiRjb20uYnNoZy5ob21lY29ubmVjdC5hbmRyb2lkLnJlbGVhc2USE2hvbWUtY29ubmVjdC1hY3Rpb24KIwoQY29tLmNhZ2xvYmFsLmlvdBIPbXktaXZhdGlvbi0yMDE5Ch8KDGNvbS5jZS5zbWFydBIPY2Utc21hcnQtYWN0aW9uCikKFmNvbS5jb2FsYXNtYXJ0LmRvbHBoaW4SD2thbWlhLWFzc2lzdGFudAolChFjb20uY29tZm9ydC5zbWFydBIQdGNsLWhvbWUtY29tZm9ydAomChBjb20uY29tZm9ydC56b25lEhJjb21mb3J0LXpvbmUtZWM3YzMKIgoQY29tLmNvbmVjdG96LmlvdBIOY29uZWN0b3otc21hcnQKJwoLY29tLmNvb2xraXQSGGV3ZWxpbmstc21hcnQtaG9tZS0zZGNjNAoxChpjb20uY3JlZWxpZ2h0aW5ndGVzdC5zbWFydBITY3JlZS1saWdodGluZy01ZWZlZAovChtjb20uY3JvbXB0b25jb2luLm15Y3JvbXB0b24SEG15Y3JvbXB0b24tNGI0NzEKKgoYY29tLmRsaW5rLm15ZGxpbmt1bmlmaWVkEg5teWRsaW5rLTE4MTAwNgosChdjb20uZWNoby5ub21hX2NocmlzdG1hcxIRbm9tYS1saWdodHMtMzRiZTQKJwoXY29tLmVjb2JlZS5hdGhlbmFtb2JpbGUSDGVjb2JlZS1mOTA2ZgozChpjb20uZWxlY3Ryb2x1eC5teWVseC50YXN0ZRIVaG9tZS1wcm9kdWN0aW9uLWVkYTgyCigKFGNvbS5lbmJyaWdodGVuLnNtYXJ0E

hBlbmJyaWdodGVuLThiZTA0CiIKE2NvbS5lbmVyanNtYXJ0LmhvbWUSC2VuZXJqLXNtYXJ0CigKEWNvbS5lc3RldmV6LnNtYXJ0EhNlc3RldmV6LXNtYXJ0LWE0NjJkCiMKE2NvbS5ldGhlcmhvb
POSSIBLE SECRETS
W0uaHlbZkISDHBkaXJvdC1kNzBkNwotChZjb20uZXVmeWxpZmUuc21hcnRob21lEhNldWZ5aG9tZS1wcm9kdWN0aW9uChgKCWNvbS5lenZpehILdGVzdDItOWZhZDMKJwoRY29tLmZpcnN0LmxpdmluZzESEmZpcnN0LWxpdmluZy03MjMwNgoiCg5jb20uZ2Uua2l0Y2hlbhIQZ2UtYXBwbGlhbmNlcy1kYQowChljb20uZ2V0b3Jyby5hbmRyb2lkY2xpZW50EhNvcnJvLXByb2QtYXNzaXN0YW50CiEKEmNvbS5nbG9iZS5lbGVjdHJpYxILZ2xvYmUtc3VpdGUKJgoRY29tLmdtbW9kWxhci5pb3QSEWdtLWtvbm5lY3QtMjM2MTAyCiAKEGNvbS5nb3N1bmQuc21hcnQSDGdvc3VuZC01OTBjMQobCgtjb20uZ3JwLm13axIMaG9tZWxhYnMtaW90CicKDmNvbS5oYW1hLnNtYXJ0EhVoYW1hLXNtYXJ0LWhvbWUtYzI5MTcKIQoIY29tLmhla2ESFWhla2Etc21hcnQtaG9tZS1iYmFlZAosChtjb20uaG9uZXl3ZWxsLmFuZHJvaWQubHlyaWMSDWx5cmljLWhhMi1kZXYKOAopY29tLmhvbmV5d2VsbC5tb2JpbGUuYW5kcm9pZC50b3RhbENvbWZvcnQSC3RjYy11ay1wcm9kChgKCmNvbS5odWFsYWkSCnd5emUtYWYzNDkKPQoeY29tLmh1c3F2YXJuYS5hdXRvbW93ZXJjb25uZWN0EhthdXRvbW93ZXItc21hcnQtaG9tZS1hY3Rpb24KHgoPY29tLmlob21lZm9yEgtpaG9tZS1jbGVhbgosChljb20uaWtlYS50cmFkZnJpLmxpZ2h0aW5nEg9pa2VhdHJhZGZyaXByb2QKKAoVY29tLmlsaWZlc21hcnQubXNsaWN0Eg9saWZlc21hcnQtM2Q5NGIKKQoVY29tLmlvdGZ5LnNtYXJ0dGhpbmdzEhBzbWFydC10aGluZy10ZXN0CiQKEmNvbS5pb3RoaW5ncy5zbWFydBIOaW90aGluZ3MtYzY0NWQKIgoSY29tLmlyaXNzbWFydC5taWFuEgxpcmlzLXNtYXJ0LWE0NjJkCiMKE2NvbS5pdGhlcmhvbWUuaHlwZXJpYmx5EgpoaXRoZXJob21lChgKEm...

POSSIBLE SECRETS

kbxIMem1vZG8tYWN0aW9uCioKGGRlLmV2ZXJob21lLmNsb3VkYm94cHJvZBIOZXZlcmhvbWUtYTY3Y2YKOgoiaW8uaG9tZWFzc2lzdGFudC5jb21wYW5pb24uYW5kcm9pZBIUaG9tZS1hc [illegible]KFgoHaW8ua2lvdBILa2lvdC0xNjQzMTAKGgoHaW8ubnVraRIPbnVraS1zbWFydC1ob21lCikKEWlvLm9saWJyYS5ib25kYXBwEhRib25kLWludGVncmF0aW9ucy12 Mgo0ChZpby5zbWFydGVuaXQuY29tcGFuaW9uEhpzbWFydGVuaXQtc21hcnRob21lLWFjdGlvbgorChRpdC5iZWVzbWFydC5hY3Rpdml0eRITc3RvcmllZC1iZWFyaW5nLTUwNQorChtqcC5j
by5oaXRhY2hpX2dscy5jb25jaWVyZ2USDGhhcHNtYXJ0aG9tZQo2ChlqcC5jby5zaGFycC5obXMuc21hcnRsaW5rEhljb2Nvcm8tYWlyLWZvci1zbWFydC1ob21lCh0KCmxpbmtvLmhvbWUSD 2xpbmtvLWlvdC0zNzc0OAohChJtMGwwX2FuZC52MjAyMF8wMDESC20wbDAtMjg2NDExCjYKFG1lLm5hbm9sZWFmLm5hbm9sZWFmEh5uYW5vbGVhZi1nYXNzaXN0YW50LXByb2R1Y3 Rpb24KIwoMbWUuc2xlZXAuYXBwEhNzbGVlcG1lLXZvaWNlLWM2Y2YyChsKCW9tLmVrby5hdRIOZWtvLWhvbWUtYjg4NWEKJQoUb3JnLm9wZW5oYWIuaGFiZHJvaWQSDW9wZW5oYWIt MjgyMDkKIQoRb3JsYS5jb25uZWN0LmhvbWUSDG9ybGEtY29ubmVjdAonCg5wYXR1bW92aWwuZG9tbxIVcGF0dW1vdmlsLWRvbW8tMzExNjEzCiQKEnNtYXJ0LmJyaXRhbmlhLmNvbRIOc 21hcnQtYnJpdGFuaWEKKAoRc21hcnQubDJocHJvYS5jb20SE2xpbmsyaG9tZS1wcm8tNThjODYKOAoYdGVjaC5icmlsbGlhbnQuYnJpbGxpYW50EhxicmlsbGlhbnQtbGlnaHQtY29udHJvbC1 wcm9kCjMKEXR3LmNvbS5haWZhLmljdHJsX3BybxIKaS1jdHJsLXByb3wogCg51bmkuVU5JN0RGQzBFNRIObXlzYWhvbWUtZjhlYjQKHgoNdmVudG90YS5jby5qcBINd2ktaG9tZS0zZDYwQQ
0e7c6160-fab2-11e4-9fbb-0002a5d5c51b
5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AAD B5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9 C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E3 1476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B0 90489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7D ED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B
22216033-F99B-412B-AFCA-670FD4BEDFF5
CgtTTUNPNjAwTlZBQwoJU01DTzYwME5WCgxTTUNPNjAwTlZBQ0EKClNNQ082MDBOVkEKA1NDNQ
077c6160-fab2-11e4-9fbb-0002a5d5c51b
097c6160-fab2-11e4-9fbb-0002a5d5c51b
1D7C6160-FAB2-11E4-9FBB-0002A5D5C51B
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
fc9dd0b3-cb84-e084-0642-f3f7e2e0bfcb
216C6160-FAB2-11E4-9FBB-0002A5D5C51B
CjBodHRwczovL25lc3QtY2FtZXJhLW1lZGlhLnNhbmRib3guZ29vZ2xlLmNvbTo0NDMKL2h0dHBzOi8vbmVzdC1jYW1lcmEtZnJvbnRlbmQuZ29vZ2xlYXBpcy5jb206NDQzCj5odHRwczovL2F 1dG9wdXNoLW5lc3RjYW1lcmFjbG91ZC1wYS5zYW5kYm94Lmdvb2dsZWFwaXMuY29tOjQ0Mw
0b7c6160-fab2-11e4-9fbb-0002a5d5c51b

POSSIBLE SECRETS
e2719d58-a985-b3c9-781a-b030af78d30e
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
GvAICvQBCu4BChphY3Rpb24uZGV2aWNlcy50eXBlcy5MSUdlVAobYWN0aW9uLmRldmljZXMudHlwZXMuU1dJVENIChthY3Rpb24uZGV2aWNlcy50eXBlcy5PVVRMRVQKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLlRIRVJNT1NUQVQKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLkFDX0hFQVRJTkcKHGFjdGlvbi5kZXZpY2VzLnR5cGVzLkFDX1VOSVQKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLkhFQVRFUgoZYWN0aW9uLmRldmljZXMudHlwZXMuTE9DSxIBKgrdAQrXAQobYWN0aW9uLmRldmljZXMudHlwZXMuQ0FNRVJBCh1hY3Rpb24uZGV2aWNlcy50eXBlcy5ET09SQkVMTCILbG9naS1jaXJjbGUiBGFybG8iE25lc3QtaG9tZS1hc3Npc3RhbnQiB215ZGxpbmsiDnN3YW5uLXNlY3VyaXR5Igtsb3JleC0yYzBiNSILc21ydGhvbWVhcHAiD3ZpcnR1YWwtdHNlLWxhYiIec21hcnQtaG9tZS1wcm9qZWN0LWZvci1jLTNmYWQzIg1oYS1mYWtlLWFnZW50EgEqCpYFCssCCiFhY3Rpb24uZGV2aWNlcy50eXBlcy5HQU1FX0NPTlNPTEUKImFjdGlvbi5kZXZpY2VzLnR5cGVzLlJFTU9URU NPTlRST0wKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLlNFVFRPUAodYWN0aW9uLmRldmljZXMudHlwZXMuU09VTkRCQVIKHGFjdGlvbi5kZXZpY2VzLnR5cGVzLlNQRUFLRVIKImFjdGlvbi5kZXZpY2VzLnR5cGVzLlNUUkVBTUlOR19CT1gKJ2FjdGlvbi5kZXZpY2VzLnR5cGVzLlNUUkVBTUlOR19TT1VOREJBUgokYWN0aW9uLmRldmljZXMudHlwZXMuU1RSUFNSU5HX1NUSUNLChxhY3Rpb24uZGV2aWNlcy50eXBlcy5TWU5DQk9YChdhY3Rpb24uZGV2aWNlcy50eXBlcy5UVhIbYWN0aW9uLmRldmljZXMudHlwZXMuHJhaXRzLk9uT2ZmEhxhY3Rpb24uZGV2aWNlcy50cmFpdHMuVm9sdW1lEiZhY3Rpb24uZGV2aWNlcy50cmFpdHMuVHJhbnNwb3J0Q29udHJvbBIjYWN0aW9uLmRldmljZXMudHJhaXRzLlJlbW90ZUNvbnRyb2wSIGFjdGlvbi5kZXZpY2VzLnRyYWl0cy5NZWRpYVN0YXRlEiNhY3Rpb24uZGV2aWNlcy50cmFpdHMuSW5wdXRTZWxlY3RvchIdYWN0aW9uLmRldmljZXMudHlwZXMuHJhaXRzLkNoYW5uZWwSG2FjdGlvbi5kZXZpY2VzLnRyYWl0cy5Nb2RlcxIdYWN0aW9uLmRldmljZXMudHlpZ2dsZXMSHGFjdGlvbi5kZXZpY2VzLnRyYWl0cy5SZWNvcmQ
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
038d641c4cd877dbb58022e98a9ee33c
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
448fa2df507764c816e7bbb286fadc75
faf69aeea3c7ebdaa7a976f27a47a17b0c3ef2b3-
F7AA99FF-7D27-4624-8CA7-C5B2760CAA80
0d7c6160-fab2-11e4-9fbb-0002a5d5c51b
157c6160-fab2-11e4-9fbb-0002a5d5c51b
658648BB-DAB5-4D4D-8E1F-0A7E0A180403
AIzaSyAEVW9QryxoI5bbSapEl9uwxt9fP77P2fg

POSSIBLE SECRETS
CiFhY3Rpb24uZGV2aWNlcy50eXBlcy5HQU1FX0NPTlNPTEUKF2FjdGlvbi5kZXZpY2VzLnR5cGVzLlRW
CidodHRwOi8vb25odWIuaGVyZS9hYm91dF9vc19jcmVkaXRzLmh0bWw
017c6160-fab2-11e4-9fbb-0002a5d5c51b
ChhOZXN0IENhbSAoaW5kb29yLCB3aXJlZCkKEk5lc3QgQ2FtIChiYXR0ZXJ5KQ
AIzaSyBmGDOmYcGmylWMKTdQxmf5vXWAuybv7qA
Ch9hY3Rpb24uZGV2aWNlcy50cmFpdHMuQXJtRGlzYXJtCiBhY3Rpb24uZGV2aWNlcy50cmFpdHMuTG9ja1VubG9jawobYWN0aW9uLmRldmljZXMudHJhaXRzLk9uT2ZmCh9hY3Rpb24uZGV2aWNlcy50cmFpdHMuT3BlbkNsb3NlCh9hY3Rpb24uZGV2aWNlcy50cmFpdHMuU3RhcnRTdG9w
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
5ae8d6093ace11e8300030d3d9752736

POSSIBLE SECRETS
CiIKEWF1LmNvbS5mb3h0ZWwuTm93Eg0vZy8xMWcwZ2JmZDVjCiYKFWF1LmNvbS5taTkuanVtcGluLmFwcBINL2cvMTFqMWx5bnY5OAoeCg9hdS5jb20uc3Rhbi5hbmQSCy9tLzAxMmZ6d3JoChsKCmNvbS5hMy5zZ3QSDS9nLzExaHMxaGo0X3cKJgoXY29tLmFwcGxlLmFuZHJvaWQubXVzaWMSCy9tLzAxM2Q3OWtuCiYKF2NvbS5hcHBsZS5hbmRyb2lkLm11c2ljEgsvbS8wMTNkNzlrbgofChBjb20uYXNwaXJvLnRpZGFsEgsvbS8wMTMwejAyZAokChNjb20uYnNicG9ydGFsLm11c2ljEg0vZy8xMWNuaHM4djM1CiQKE2NvbS5ic2Jwb3J0YWwubXVzaWMSDS9nLzExY25oczh2MzUKNgolY29tLmJ5ZGVsdXhlLmQzLmFuZHJvaWQucHJvZ3JhbS5zdGFyehINL2cvMTFoYm55ejhfawooChdjb20uY2FuYWwuYW5kcm9pZC5jYW5hbBINL2cvMTFmeTl5NWM1NQobCgtjb20uY2JzLmFwcBIML2cvMXE2czdxenp0CiMKFWNvbS5jaGFubmVsNC5vbmRlbWFuZBIKL20vMGgzbXI3XwomChVjb20uZGlzbmV5LmRpc25leXBsdXMSDS9nLzExZmtua25yZGcKIgoRY29tLmVwaXguZXBpeC5ub3cSDS9nLzExZnI2MzZidGcKKAoYY29tLmV6cGVlci5lenBlZXJwbHVzLnY0EgwvZy8xMXJfcGt3ZjgKFwoJY29tLmdhYW5hEgovbS8wcnBmazF2ChcKCWNvbS5nYWFuYRIKL20vMHJwZmsxdgoiChFjb20uZ2xvYm8uZ2xvYm90dhINL2cvMTFnaHFjancwMwo1CiRjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy55b3V0dWJlLmtpZHMSDS9nLzExZHltdjB5YmIKNQokY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMueW91dHViZS5raWRzEg0vZy8xMWR5bXYweWJiCjIKJWNvbS5nb29nbGUuYW5kcm9pZC5hcHBzLnlvdXR1YmUubXVzaWMSCS9tLzA5amN2cwofCg5jb20uaGJvLmhib25vdxINL2cvMTFqZmRkZjExMwodCg1jb20uaHVsdS5wbHVzEgwvZy8xcTZzMmtfeXEKLAobY29tLmh1bmdhbWEubXlwbGF5LmFjdGl2aXR5Eg0vZy8xMWJ5Y2R3eHZ0CiwKG2NvbS5odW5nYW1hLm15cGxheS5hY3Rpdml0eRINL2cvMTFieWNkd3h2dAokChZjb20uamlvLm1lZGlhLmppb2JlYXRzEgovbS8wNDd0amgwCiQKFmNvbS5qaW8ubWVkaWEuamlvYmVhdHMSCi9tLzA0N3RqaDAKKQobY29tLmppby5tZWRpYS5qaW9iZWF0cy5saXRlEgovbS8wNDd0amgwCicKFmNvbS5rdG11c2ljLmdlbmllbXVzaWMSDS9nLzExY25oczJzMGYKKAoXY29tLm5lb3dpei5hbmRyb2lkLmJ1Z3MSDS9nLzExZzBsbDgydDEKJwoXY29tLm5ldGZsaXgubWVkaWFjbGllbnQSDC9nLzFxNnMxeHZkeAosChtjb20ubnR0ZG9jb21vLmFuZHJvaWQuZGhpdHMSDS9nLzExZ3l5YnF6XzgKIAoTY29tLnBhbmRvcmEuYW5kcm9pZBIJL20vMDkxemdtCh0KDWNvbS5wYnMudmlkZW8SDC9nLzFxNnM2cHhmcgofChFjb20uc2Fhdm4uYW5kcm9pZBIKL20vMDQ3dGpoMAobCgpjb20uc2lyaXVzEg0vZy8xMWZqeHd6XzdqCioKGWNvbS5za3lzb2Z0LmtrYm94LmFuZHJvaWQSDS9nLzExaDNxcWRmejIKGgoJY29tLnNsaW5nEg0vZy8xMWY2Mzd5c2ZuCiQKFmNvbS5zb3VuZGNsb3VkLmFuZHJvaWQSCi9tLzA0enhtcjgKHwoRY29tLnNwb3RpZnkubXVzaWMSCi9tLzA0eWhkNmMKKQoYY29tLnRhaXdhbm1vYmlsZS5teVZpZGVvEg0vZy8xMWo1M204ZGo1Ci0KHGNvbS50ZWxlY29taXRhbGlhLmN1Ym9tdXNpY2ESDS9nLzExajM2d2ZuNDEKJQoUY29tLnRlbmNlbnQuaWJnLmpvb3gSDS9nLzExYndnNzlsZ2oKGwoKY29tLnR1YmltdhINL2cvMTFnZmo3bHN2ZgokChNjb20udmlhcGxheS5hbmRyb2lkEg0vZy8xMWcwaHB6Z3hyCh4KEGNvbS52aWtpLmFuZHJvaWQSCi9tLzBqbDFnMzIKHgoQY29tLnZpa2kuY W5kcm9pZBIKL20vMGpsMWczMgoiChFjb20uemF0dG9vLnBsYXllchINL2cvMTFnZHlqN2J3dAonChZkZS5tYXhkb21lLmFwcC5hbmRyb2lkEg0vZy8xMWc5cTQ4NTI1CiAKEmRlZXplci5hbmRyb2lkLmFwcBIKL20vMDNjMmNrZAohChBmbS5hd2EubGl2ZXJwb29sEg0vZy8xMWdibGR6bnNfCigKF2luLnN0YXJ0di5ob3RzdGFyLmRwbHVzEg0vZy8xMXI0YmNrZjV2CicKFml0Lm1lZGlhc2V0LmluZmluaXR5dHYSDS9nLzExaDNiZ21zMWQKGgoJaXQucmFpbmV0Eg0vZy8xMWgzc3IyYzBzCiwKG2l0LnRlbGVjb21pdGFsaWEuY3Vib3Zpc2lvbhINL2cvMTFmc3pfZjNmdwojChNqcC5jby5udHRkb2NvbW8uZHR2EgwvZy8xMmhoZ3k5ZjMKIwoSanAuaGFwcHlvbi5hbmRyb2lkEg0vZy8xMWYxMGR4dHNfCi4KHWpwLmxpbmVjb3JwLmxpbmVtdXNpYy5hbmRyb2lkEg0vZy8xMWo4bjBkbXQ1CiUKFGpwLnVuZXh0Lm1lZGlhcGxheWVyEg0vZy8xMWZrMW50ang3CiMKEmtyLmNvLmNhcHR2LnBvb3FWMhINL2cvMTFmdDY4dzVucAoyCiFuei5jby50dm56Lm9uZGVtYW5kLnBob25lLmFuZHJvaWQSDS9nLzExajExMDNibmgKIwoSc2twbGFuZXQubXVzaWNtYXRlEg0vZy8xMWo4aGxrNTR4Ch8KDnR2Lm1vbG90b3YuYXBwEg0vZy8xMWYxNDZkdjRt
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
9FF50B39-76B6-499F-BEBF-CC04B0CE8C18
F098507F-3ED2-45B5-84F9-824FAD00BA40
076aa300-0576-11e5-b9a5-0002a5d5c51b
1b6c6160-fab2-11e4-9fbb-0002a5d5c51b
177c6160-fab2-11e4-9fbb-0002a5d5c51b

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
6EA5992F-3DEE-4481-929A-3DC73EFA3C23
137c6160-fab2-11e4-9fbb-0002a5d5c51b
217C6160-FAB2-11E4-9FBB-0002A5D5C51B
GqIKCsgCCsICChphY3Rpb24uZGV2aWNlcy50eXBlcy5MSUdlVAobYWN0aW9uLmRldmljZXMudHlwZXMuU1dJVENIChthY3Rpb24uZGV2aWNlcy50eXBlcy5PVVRMRVQKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLlRlRVJNT1NUQVQKH2FjdGlvbi5kZXZpY2VzLnR5cGVzLkHGFjdGlvbi5kZXZpY2VzLnR5cGVzLkFDX1VOSVQKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLkhFQVRFUgobYWN0aW9uLmRldmljZXMudHlwZXMuS0VUVExFChhhY3Rpb24uZGV2aWNlcy50eXBlcy5NT1AKG2FjdGlvbi5kZXZpY2VzLnR5cGVzLlZBQ1VVTQoZYWN0aW9uLmRldmljZXMudHlwZXMuTE9DSxIBKgrOAQrIAQobYWN0aW9uLmRldmljZXMudHlwZXMuQ0FNRVJBCh1hY3Rpb24uZGV2aWNlcy50eXBlcy5ET09SQkVMTCILbG9naS1jaXJjbGUiBGFybG8iE25lc3QtaG9tZS1hc3Npc3RhbnQiB215ZGxpbmsiDnN3YW5uLXNlY3VyaXR5Igtsb3JleC0yYzBiNSILc21ydGhvbWVhcHAiD3ZpcnR1YWwwtdHNlLWxhYiIec21hcnQtaG9tZS1wcm9qZWN0LWZvci1jLTNmYWQzEgEqCmsKZgocYWN0aW9uLmRldmljZXMudHlwZXMuRElTUExBWSIjZ29vZ2xlLmNvbTphcGktcHJvamVjdC00OTg1Nzk2MzM1MTQqDE5lc3QgSHViIE1heCoTR29vZ2xlIE5lc3QgSHViIE1heBIBKgqWBQrLAgohYWN0aW9uLmRldmljZXMudHlwZXMuR0FNRV9DT05TT0xFCiJhY3Rpb24uZGV2aWNlcy50eXBlcy5SRU1PVEVDT05UUk9MChthY3Rpb24uZGV2aWNlcy50eXBlcy5TRVRUT1AKHWFjdGlvbi5kZXZpY2VzLnR5cGVzLlNPVU5EQkFSChxhY3Rpb24uZGV2aWNlcy50eXBlcy5TUEVBS0VSCiJhY3Rpb24uZGV2aWNlcy50eXBlcy5TVFJFQU1JTkdfQk9YCidhY3Rpb24uZGV2aWNlcy50eXBlcy5TVFJFQU1JTkdfU09VTkRCQVIKJGFjdGlvbi5kZXZpY2VzLnR5cGVzLlNUUkVBTUlOR19TVElDSwocYWN0aW9uLmRldmljZXMudHlwZXMuU1lOQ0JPWAoXYWN0aW9uLmRldmljZXMudHlwZXMuVFYSG2FjdGlvbi5kZXZpY2VzLnRyYWl0cy5Pbk9mZhIcYWN0aW9uLmRldmljZXMudHlwZXMuVFZRImYWN0aW9uLmRldmljZXMudHlwZXMuRlRyYW5zcG9ydENvbnRyb2wSI2FjdGlvbi5kZXZpY2VzLnRyYWl0cy5SZW1vdGVDb250cm9sEiBhY3Rpb24uZGV2aWNlcy50cmFpdHMuTWVkaWFTdGF0ZRIjYWN0aW9uLmRldmljZXMudHlwZXMuRlRyYW5zcG9ydENvbnRyb2wSHWFjdGlvbi5kZXZpY2VzLnRyYWl0cy5DaGFubmVsEhthY3Rpb24uZGV2aWNlcy50cmFpdHMuTW9kZXMSHWFjdGlvbi5kZXZpY2VzLnRyYWl0cy5Ub2dnbGVzEhxhY3Rpb24uZGV2aWNlcy50cmFpdHMuUmVjb3Jk
196c6160-fab2-11e4-9fbb-0002a5d5c51b
C3938289-DE82-44F8-B11C-3773241502DC
147c6160-fab2-11e4-9fbb-0002a5d5c51b
86254750241babac4b8d52996a675549
3D26DE21-5DD5-483E-9FAF-FA1CEC89A7DE
B5257ED2-12CC-4C83-84B8-C10B7AC80BA7
01cb7134e1275fc4fd133e1b9de85c5a

POSSIBLE SECRETS
f8c81f8c1d0669e53ef63c6b89097a1d
d44e4be256518704d4e3ee4b6b089c9f
90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73
156c6160-fab2-11e4-9fbb-0002a5d5c51b
1c6c6160-fab2-11e4-9fbb-0002a5d5c51b
0a7c6160-fab2-11e4-9fbb-0002a5d5c51b
276C6160-FAB2-11E4-9FBB-0002A5D5C51B
AIzaSyC8UYZpvA2eknNex0Pjid0
Ci1jb20uZ29vZ2xlLmFuZHJvaWQucHJpbWVzLWphbmstJVBBQ0tBR0VfTkFNRSUSIwgCEh9KPCVFVkVOVF9OQU1FJT4jbWlzc2VkQXBwRnJhbWVzEh8IAxIbSjwlRVZFTlRfTkFNRSU+I3RvdGFsRnJhbWVzEiYIBRIiSjwlRVZFTlRfTkFNRSU+I21heEZyYW1lVGltZU1pbGxpcw
c5e7d25a0e7030289897dda2ecd46001
F0C3B13F-6AED-46EA-BEAA-0C7A11B1F02D
D3D14F85-133D-4F19-A1C1-A471B2C23826
026DD092-CB00-45B2-8DBB-77D8897F0493
2B7C6160-FAB2-11E4-9FBB-0002A5D5C51B

POSSIBLE SECRETS
cf66d89d29f160a56452e1ec819be807
CqICChIKBWRlLURFEglEdXJjaHNhZ2UKEgoFZGUtQVQSCUR1cmNoc2FnZQoSCgVlbi1VUxIJQnJvYWRjYXN0ChIKBWVuLUdCEglCcm9hZGNhc3QKEgoFZW4tQVUSCUJyb2FkY2FzdAoSCgVlbi1DQRIJQnJvYWRjYXN0ChIKBWVuLUlOEglCcm9hZGNhc3QKEgoFZW4tU0cSCUJyb2FkY2FzdAoTCgVmci1GUhIKTcOpZ2FwaG9uZQoTCgVmci1DQRIKTcOpZ2FwaG9uZQoRCgVpdC1JVBIIQW5udW5jaW8KDwoFZXMtRVMSBkVtaXRpcgoPCgVlcy1VUxIGRW1pdGlyCiEKBWphLUpQEhjjg5bjg63jg7zjg4njgq3jg6Pjgrnjg4g
1b7c6160-fab2-11e4-9fbb-0002a5d5c51b

PLAYSTORE INFORMATION

Title: Google Home

Score: 4.098488 **Installs:** 1,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** com.google.android.apps.chromecast.app

Developer Details: Google LLC, 5700313618786177705, None, http://cast.google.com/chromecast/, apps-help@google.com,

Release Date: Jul 18, 2013 **Privacy Policy:** Privacy link

Description:

The Google Home app helps you get the most out of Gemini for Home. See your home at a glance The Google Home app is designed to show you the status of your home and keep you up to date with what you may have missed. Keep up with what's important Updated design and streamlined organization help you group your devices into dashboards and easily navigate your settings. Plus you can check in on your home anytime. Scan camera events quickly The camera live view and history interface makes it easier than ever to see what happened. Search or ask your home Control your home in a brand new way. Just say what you want your devices to do with Gemini for Home. * Some products and features may not be available in all regions. Compatible devices required.

SCAN LOGS

Timestamp	Event	Error
2026-01-03 06:05:13	Generating Hashes	OK

2026-01-03 06:05:13	Extracting APK	OK
2026-01-03 06:05:13	Unzipping	OK
2026-01-03 06:05:14	Parsing APK with androguard	OK
2026-01-03 06:05:14	Extracting APK features using aapt/aapt2	OK
2026-01-03 06:05:14	Getting Hardcoded Certificates/Keystores	OK
2026-01-03 06:05:16	Parsing AndroidManifest.xml	OK
2026-01-03 06:05:16	Extracting Manifest Data	OK
2026-01-03 06:05:16	Manifest Analysis Started	OK
2026-01-03 06:05:16	Reading Network Security config from network_security_config.xml	OK
2026-01-03 06:05:16	Parsing Network Security config	OK
2026-01-03 06:05:16	Performing Static Analysis on: Home (com.google.android.apps.chromecast.app)	OK
2026-01-03 06:05:16	Fetching Details from Play Store: com.google.android.apps.chromecast.app	OK

2026-01-03 06:05:17	Checking for Malware Permissions	OK
2026-01-03 06:05:17	Fetching icon path	OK
2026-01-03 06:05:17	Library Binary Analysis Started	OK
2026-01-03 06:05:17	Reading Code Signing Certificate	OK
2026-01-03 06:05:17	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/ef3419cd44e8a8ddf575a1133977fde1/ef3419cd44e8a8ddf575a1133977fde1.apk'])
2026-01-03 06:05:17	Running APKiD 3.0.0	OK
2026-01-03 06:05:21	Detecting Trackers	OK
2026-01-03 06:05:22	Decompiling APK to Java with JADX	OK
2026-01-03 06:05:40	Converting DEX to Smali	OK
2026-01-03 06:05:40	Code Analysis Started on - java_source	OK
2026-01-03 06:05:46	Android SBOM Analysis Completed	OK

2026-01-03 06:05:51	Android SAST Completed	OK
2026-01-03 06:05:51	Android API Analysis Started	OK
2026-01-03 06:05:56	Android API Analysis Completed	OK
2026-01-03 06:05:56	Android Permission Mapping Started	OK
2026-01-03 06:06:56	Android Permission Mapping Completed	OK
2026-01-03 06:06:57	Android Behaviour Analysis Started	OK
2026-01-03 06:07:06	Android Behaviour Analysis Completed	OK
2026-01-03 06:07:06	Extracting Emails and URLs from Source Code	OK
2026-01-03 06:07:14	Email and URL Extraction Completed	OK
2026-01-03 06:07:14	Extracting String data from APK	OK
2026-01-03 06:07:14	Extracting String data from Code	OK
2026-01-03 06:07:14	Extracting String values and entropies from Code	OK

2026-01-03 06:07:16	Performing Malware check on extracted domains	OK
2026-01-03 06:07:21	Saving to Database	OK

Report Generated by - MobSF v4.4.4

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.