MOBSF

ANDROID STATIC ANALYSIS REPORT

Drive (2.21.241.10.40)

File Name:	Drive.apk
Package Name:	com.google.android.apps.docs
Scan Date:	March 10, 2024, 6:34 a.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	73	0	1	1

FILE INFORMATION

File Name: Drive.apk
Size: 55.88MB
MD5: e905b00e6c7a3401ba9c05ee060dc443
SHA1: e91e732f6ed4e650fea060061e271f43c8e81294
SHA256: be509759d55f46b64e4fdfc5d74d6b608eedc3c49350099060de9a5dad0bbe32

APP INFORMATION

App Name: Drive
Package Name: com.google.android.apps.docs
Main Activity: com.google.android.apps.docs.preferences.DocsPreferencesActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 2.21.241.10.40

Android Version Code: 212411040

APP COMPONENTS

Activities: 86
Services: 28
Receivers: 28
Providers: 13
Exported Activities: 35
Exported Services: 4
Exported Receivers: 22
Exported Providers: 6

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-08-21 23:13:34+00:00
Valid To: 2036-01-07 23:13:34+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc2e08746644a308d
Hash Algorithm: md5
md5: cde9f6208d672b54b1dacc0b7029f5eb
sha1: 38918a453d07199354f8b19af05ec6562ced5788
sha256: f0fd6c5b410f25cb25c3b53346c8972fae30f8ee7411df910480ad6b2d60db83
sha512: edf99db872937471eb94cbe576512a0089527e28b5b65df96f18f539737955ef1ce2553a51156ee31b521dcdc1559c52e965899f13038487d03743742b634326
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 843817f137559b510590075c0256a414a5767c6f32f91a46228077c065ba67fe
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.SUBSCRIBED_FEEDS_READ	normal	read subscribed feeds	Allows an application to receive details about the currently synced feeds.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SUBSCRIBED_FEEDS_WRITE	dangerous	write subscribed feeds	Allows an application to modify your currently synced feeds. This could allow a malicious application to change your synced feeds.
com.google.android.gm.permission.READ_GMAIL	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googleapps.permission.GOOGLE_AUTH	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googleapps.permission.GOOGLE_AUTH.OTHER_SERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googleapps.permission.GOOGLE_AUTH.ALL_SERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googleapps.permission.GOOGLE_AUTH.writely	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googleapps.permission.GOOGLE_AUTH.wise	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.apps.docs.permission.READ_MY_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.apps.docs.permission.SYNC_STATUS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.apps.docs.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/e905b00e6c7a3401ba9c05ee060dc443/e905b00e6c7a3401ba9c05ee060dc443.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Obfuscator</td><td>DexGuard</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT 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>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
possible Build.SERIAL check
Build.TAGS 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>classes3.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>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.apps.docs.openurl.DriveOpenUrlActivityAlias	Schemes: http://, https://, Hosts: drive.google.com, icing.drive.google.com, docs.google.com, Path Patterns: /, /a/.*/, /m, /a/.*/m, /folder.*, /a/.*/folder.*, /file/.*, /a/.*/file/.*, /open, /a/.*/open, /leaf, /a/.*/leaf, /uc, /a/.*/uc, /viewer, /a/.*/viewer,
com.google.android.apps.docs.openurl.KixOpenUrlActivityAlias	Schemes: http://, https://, Hosts: docs.google.com, Path Patterns: /document/.*, /a/.*/document/.*, /Doc, /a/.*/Doc, /View, /a/.*/View,
com.google.android.apps.docs.openurl.TrixOpenUrlActivityAlias	Schemes: http://, https://, Hosts: docs.google.com, spreadsheets.google.com, Path Patterns: /spreadsheets/.*, /spreadsheet/.*, /a/.*/spreadsheet/.*, /spreadsheets/d/.*, /a/.*/spreadsheets/d/.*,
com.google.android.apps.docs.openurl.PunchOpenUrlActivityAlias	Schemes: http://, https://, Hosts: docs.google.com, Path Patterns: /present/.*, /a/.*/present/.*, /presentation/.*, /a/.*/presentation/.*,
com.google.android.apps.viewer.PdfViewerActivity	Schemes: file://, content://, http://, https://, Hosts: *, Mime Types: application/pdf, Path Patterns: .*\\.pdf,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

NO	SCOPE	SEVERITY	DESCRIPTION
2	*	warning	Base config is configured to trust system certificates.
3	googleapis.com google.com google.cn gvt1.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 69 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
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	Activity (com.google.android.apps.docs.drive.startup.StartupActivity) 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
6	Activity-Alias (com.google.android.apps.docs.drive.NotificationsCenterAliasActivity) 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.
7	Activity-Alias (com.google.android.apps.docs.app.NewMainProxyActivity) 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.docs.app.OpenSafUrlActivity) 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	Content Provider (com.google.android.apps.docs.common.sync.filemanager.FileProvider) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Content Provider (com.google.android.apps.docs.storagebackend.StorageBackendContentProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.MANAGE_DOCUMENTS [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. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Content Provider (com.google.android.apps.docs.storagebackend.LegacyStorageBackendContentProvider) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Activity-Alias (com.google.android.apps.docs.GlobalSearch) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.GLOBAL_SEARCH [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. 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.
13	Activity (com.google.android.apps.docs.common.shareitem.UploadMenuActivity) 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
14	Activity-Alias (com.google.android.apps.docs.app.GetContentActivity) 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.
15	Activity-Alias (com.google.android.apps.docs.app.PickActivity) 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.
16	Activity-Alias (com.google.android.apps.docs.app.DocumentOpenerActivityProxy) 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.
17	Activity (com.google.android.apps.docs.drive.openurl.OpenUrlActivity) 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
18	Activity-Alias (com.google.android.apps.docs.openurl.OpenUrlActivity) 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.
19	Activity-Alias (com.google.android.apps.docs.openurl.DriveOpenUrlActivityAlias) 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.
20	Activity-Alias (com.google.android.apps.docs.openurl.KixOpenUrlActivityAlias) 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.
21	Activity-Alias (com.google.android.apps.docs.openurl.TrixOpenUrlActivityAlias) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
22	Activity-Alias (com.google.android.apps.docs.openurl.PunchOpenUrlActivityAlias) 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.
23	Activity-Alias (com.google.android.apps.docs.app.PaymentsActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
24	Broadcast Receiver (com.google.android.apps.docs.drive.appindexing.AppIndexingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.APPINDEXING [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.
25	Broadcast Receiver (com.google.android.apps.docs.notification.common.NotificationBanReceiver) 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
26	Service (com.google.android.apps.docs.drive.ipcservice.DriveIpcService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
27	Activity (com.google.android.apps.docs.common.androidshortcuts.CreateShortcutActivity) 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.
28	Activity-Alias (com.google.android.apps.docs.androidshortcuts.CreateShortcutActivity) 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.
29	Activity (com.google.android.apps.docs.common.androidshortcuts.CreateDocumentScanShortcutActivity) 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
30	Activity-Alias (com.google.android.apps.docs.androidshortcuts.CreateDocumentScanShortcutActivity) 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.
31	Activity (com.google.android.apps.docs.common.androidshortcuts.ScanToDriveActivity) 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.
32	Activity-Alias (com.google.android.apps.docs.shortcut.ScanToDriveActivity) 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.
33	Activity-Alias (com.google.android.apps.docs.androidshortcuts.ScanToDriveActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
34	Content Provider (com.google.android.apps.docs.doclist.DocListGlobalSearchSuggestionProvider) is Protected by a permission. Permission: com.google.android.apps.docs.permission.READ_MY_DATA protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
35	Content Provider (com.google.android.apps.docs.common.welcome.PromotionEnabled) 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.
36	Service (com.google.android.apps.docs.common.sync.syncadapter.DocsSyncAdapterService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
37	TaskAffinity is set for activity (com.google.android.apps.docs.print.PrintActivity)	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.
38	Activity-Alias (com.google.android.apps.docs.app.detailpanel.DetailActivity) 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.
39	Activity (com.google.android.apps.docs.help.HelpMenuTrampolineActivity) 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
40	Activity (com.google.android.apps.docs.help.ReportAbuseActivity) 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	Broadcast Receiver (com.google.android.apps.docs.doclist.statesyncer.CrossAppStateChangedEventReceiver) 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.
42	Broadcast Receiver (com.google.android.apps.docs.doclist.statesyncer.DocumentContentStatusChangedReceiver) 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.
43	Broadcast Receiver (com.google.android.apps.docs.download.DownloadManagerReceiver) 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
44	Content Provider (com.google.android.apps.docs.doclist.statesyncer.CrossAppStateProvider) 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.
45	Activity (com.google.android.apps.docs.drive.clipboard.SendTextToClipboardActivity) 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.
46	Service (com.google.android.apps.docs.drive.devtools.DeveloperToolsService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
47	Activity (com.google.android.apps.docs.drive.filepicker.GetMetadataActivity) 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
48	Content Provider (com.google.android.apps.docs.drive.slices.DriveSliceProvider) 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.
49	Activity (com.google.android.apps.docs.drive.widget.WidgetConfigureActivity) 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.
50	Broadcast Receiver (com.google.android.apps.docs.drive.widget.CakemixAppWidgetProvider) 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
51	Broadcast Receiver (com.google.android.apps.docs.notification.guns.GcmBroadcastReceiver) 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.
52	Activity (com.google.android.apps.docs.notification.impl.ExportedNotificationHomeActivity) 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
53	Broadcast Receiver (com.google.android.apps.docs.notification.common.NotificationChannelReceiver) 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.
54	Activity (com.google.android.apps.viewer.ProjectorActivity) 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.
55	Activity (com.google.android.apps.viewer.PdfViewerActivity) 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.
56	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) 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
57	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.
58	Activity (com.google.android.libraries.abuse.reporting.ReportAbuseActivity) 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
59	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.inject.GrowthKitBootCompletedBroadcastReceiver) 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.
60	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.
61	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.internal.experiments.impl.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.
62	Broadcast Receiver (com.google.android.libraries.notifications.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.

NO	ISSUE	SEVERITY	DESCRIPTION
63	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.
64	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.gcm.GcmBroadcastReceiver) 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
65	Broadcast Receiver (com.google.android.libraries.notifications.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.
66	Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.phenotype.PhenotypeUpdateReceiver) 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.
67	Broadcast Receiver (com.google.android.libraries.notifications.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.
68	Broadcast Receiver (com.google.android.libraries.notifications.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.

NO	ISSUE	SEVERITY	DESCRIPTION
69	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.
70	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.

NO	ISSUE	SEVERITY	DESCRIPTION
71	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.
72	Activity (com.google.android.libraries.surveys.internal.view.SurveyActivity) 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
73	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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libframesequence.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libfoxit.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/librectifier.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libcello_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libbitmap_parcel.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libdocscanner_image.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libframesequence.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libfoxit.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/librectifier.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libcello_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libbitmap_parcel.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libdocscanner_image.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/24	android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/45	com.android.launcher.permission.INSTALL_SHORTCUT, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_INSTALL_PACKAGES

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
script.google.com	ok	**IP:** 172.253.118.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
preprod-driveactivity.corp.googleapis.com	ok	**IP:** 74.125.24.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cse.s	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 142.251.175.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
staging-cloudsearch.sandbox.googleapis.com	ok	**IP:** 64.233.170.81 **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:** 74.125.200.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.google.com	ok	**IP:** 74.125.68.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
staging-drivequal-driveactivity.sandbox.googleapis.com	ok	**IP:** 172.253.118.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
symbolize.corp.google.com	ok	**IP:** 172.217.194.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
staging-www.sandbox.googleapis.com	ok	**IP:** 64.233.170.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
driveactivity.googleapis.com	ok	**IP:** 74.125.68.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lh3.googleusercontent.com	ok	**IP:** 74.125.130.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
drive.sandbox.google.com	ok	**IP:** 74.125.68.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
test-www.sandbox.googleapis.com	ok	**IP:** 74.125.200.81 **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.
drive.google.com	ok	**IP:** 64.233.170.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.sandbox.google.com	ok	**IP:** 64.233.170.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
daily-cloudsearch.sandbox.googleapis.com	ok	**IP:** 142.251.10.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
com-cakemix.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
krahsc.google.com	ok	**IP:** 172.253.118.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
drive-qa.corp.google.com	ok	**IP:** 74.125.24.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cloudsearch.googleapis.com	ok	**IP:** 74.125.24.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
appsitemsuggest-pa.googleapis.com	ok	**IP:** 64.233.170.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dev-driveactivity.corp.googleapis.com	ok	**IP:** 74.125.24.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs-qa.corp.google.com	ok	**IP:** 142.251.12.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://com-cakemix.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
cakemix-db-dump@google.com cakemix-db-dump@google.com■ □cakemix-db-dump@google.com cakemix-offline@google.com cakemix-db-dump@google.com□ ne-cakemix-db-dump@google.com	Android String Resource
docs-release@ugcr5.prod	lib/arm64-v8a/libfoxit.so
docs-release@ugcr5.prod	lib/arm64-v8a/librectifier.so
appro@openssl.org docs-release@ugcr5.prod	lib/arm64-v8a/libcello_native.so
docs-release@ugcr5.prod	apktool_out/lib/arm64-v8a/libfoxit.so
docs-release@ugcr5.prod	apktool_out/lib/arm64-v8a/librectifier.so
appro@openssl.org docs-release@ugcr5.prod	apktool_out/lib/arm64-v8a/libcello_native.so

TRACKERS

TRACKER	CATEGORIES	URL

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "Nafnlaus"
"notify_heading_anonymous_user" : "ناشناس"
"ds_pdf_paper_size_key" : "ds_pdf_paper_size_key"
"notify_heading_anonymous_user" : "□□"
"notify_heading_anonymous_user" : "■■■■"
"private_link_description" : "□□□□□□□□□□□□"
"desc_password" : "lösenordsfält"
"desc_password" : "wagwoordveld"
"sharing_option_private_heading" : "Restricționat"
"notify_heading_anonymous_user" : "ანონიმური"
"notify_heading_anonymous_user" : "Anonimas"

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "Anonymous"
"notify_heading_anonymous_user" : "Anonym"
"sharing_option_private" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"sharing_option_private_heading" : "Begrenset"
"getting_authentication_information" : "□□□□□□□□□□□□□"
"notify_heading_anonymous_user" : "Anonyme"
"private_link_description" : "□□□□□□□□□□□□□"
"notify_heading_anonymous_user" : "אנונימי"
"notify_heading_anonymous_user" : "Ананім"
"notify_heading_anonymous_user" : "Okungaziwa"
"notify_heading_anonymous_user" : "□□"
"notify_heading_anonymous_user" : "Anonyymi"
"sharing_option_private_heading" : "Imedhibitiwa"
"sharing_option_private_heading" : "Beperkt"
"sharing_option_private_heading" : "□□□□□□"

POSSIBLE SECRETS
"sharing_option_private_heading" : "[redacted]"
"firebase_database_url" : "https://com-cakemix.firebaseio.com"
"sharing_option_private_heading" : "Restringit"
"sharing_option_private_heading" : "Beperk"
"notify_heading_anonymous_user" : "[redacted]"
"sharing_option_private_heading" : "Kısıtlanmış"
"sharing_option_private_heading" : "Omejeno"
"private_link_description" : "[redacted]"
"desc_password" : "passordfelt"
"sharing_option_private_heading" : "[redacted]"
"sharing_option_private_heading" : "Məhdudlaşdırılıb"
"sharing_option_private_heading" : "Murriztua"
"sharing_option_private" : "[redacted]"
"sharing_option_private_heading" : "შეზღუდული"
"notify_heading_anonymous_user" : "Анонимно"

POSSIBLE SECRETS
"sharing_option_private_heading" : "Ograničeno"
"sharing_option_private_heading" : "Restricted"
"sharing_option_private_heading" : "[redacted]"
"notify_heading_anonymous_user" : "[redacted]"
"private_link_description" : "[redacted]"
"desc_password" : "salasanakenttä"
"desc_password" : "jelszómező"
"notify_heading_anonymous_user" : "Anónimo"
"notify_heading_anonymous_user" : "[redacted]"
"sharing_option_private" : "□□□□□□□□□□□□□□□□□□□□"
"sharing_option_private_heading" : "Terhad"
"notify_heading_anonymous_user" : "□□-□□□"
"sharing_option_private_heading" : "ممنوع"
"ds_jpeg_quality_key" : "ds_jpeg_quality_key"
"sharing_option_private_heading" : "Korlátozott"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyBCcTM_PYMJ688Njw7NxBTh2DutdYNROrQ"
"notify_heading_anonymous_user" : "Анонім"
"notify_heading_anonymous_user" : "[redacted]"
"sharing_option_private_heading" : "[redacted]"
"desc_password" : "ຂ່ອງລະຫັດຜ່ານ"
"sharing_option_private_heading" : "[redacted]"
"sharing_option_private_heading" : "Eingeschränkt"
"sharing_option_private_heading" : "Хязгаарласан"
"sharing_option_private_heading" : "Restringido"
"notify_heading_anonymous_user" : "Анонимді"
"sharing_option_private_heading" : "Omezené"
"ds_display_real_time_quads_key" : "display_real_time_quads_key"
"notify_heading_anonymous_user" : "Anonüümne"
"notify_heading_anonymous_user" : "[redacted]"
"getting_authentication_information" : "□□□□□□"

POSSIBLE SECRETS
"sharing_option_private_heading" : "■■■■■■■■■■■■■■■"
"sharing_option_private_heading" : "Limitato"
"sharing_option_private_heading" : "Takmarkað"
"notify_heading_anonymous_user" : "Névtelen"
"sharing_option_private_heading" : "Limitado"
"sharing_option_private" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"ds_pdf_paper_orientation_key" : "ds_pdf_paper_orientation_key"
"notify_heading_anonymous_user" : "ບໍ່ລະບຸຊື່"
"notify_heading_anonymous_user" : "■■■■■■"
"notify_heading_anonymous_user" : "مجهول"
"sharing_option_private_heading" : "Restrito"
"sharing_option_private_heading" : "Obmedzené"
"notify_heading_anonymous_user" : "■■■■■■"
"sharing_option_private_heading" : "Rajoitettu"
"notify_heading_anonymous_user" : "Anònim"

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "[redacted]"
"getting_authentication_information" : "[redacted]"
"private_link_description" : "□□□□□□□□□□□□□□□□"
"getting_authentication_information" : "□□□□□□□"
"ds_image_enhancement_method_key" : "image_enhancement_key"
"sharing_option_private_heading" : "Шектелген"
"notify_heading_anonymous_user" : "Anonimno"
"sharing_option_private_heading" : "Սահմանափակ"
"sharing_option_private_heading" : "[redacted]"
"notify_heading_anonymous_user" : "Anonimoa"
"sharing_option_private_heading" : "Limité"
"sharing_option_private_heading" : "Ограничено"
"sharing_option_private_heading" : "Begrænset"
"sharing_option_private_heading" : "จำกัด"
"notify_heading_anonymous_user" : "Anônimo"

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "Anonim"
"sharing_option_private_heading" : "□□"
"desc_password" : "■■■■■■■■■■■■■■■■"
"sharing_option_private_heading" : "Ierobežots"
"desc_password" : "□□□□□□□"
"sharing_option_private_heading" : "■■■■■■■■■■"
"sharing_option_private_heading" : "מוגבל"
"desc_password" : "adgangskodefelt"
"private_link_description" : "ສະເພາະຄົນທີ່ເພີ່ມເຂົ້າມາທີ່ສາມາດເປີດໄດ້"
"sharing_option_private_heading" : "□□□"
"sharing_option_private_heading" : "□□□□"
"sharing_option_private" : "□□□□□□□□□□□□□□□□□□□□□□"
"notify_heading_anonymous_user" : "■■■■■■"
"sharing_option_private_heading" : "□□□"
"getting_authentication_information" : "■■■■■■■■■■■■"

POSSIBLE SECRETS
"private_link_description" : "[redacted]"
"sharing_option_private_heading" : "[redacted]"
"sharing_option_private_heading" : "Περιορισμένο"
"sharing_option_private" : "ມີຜຽງຄົນທີ່ຖືກເຜີ່ມໃສ່ທີ່ສາມາດເປີດດ້ວຍລິ້ງນີ້ໄດ້"
"notify_heading_anonymous_user" : "Anoniem"
"desc_password" : "wachtwoordveld"
"desc_password" : "[redacted]"
"notify_heading_anonymous_user" : "[redacted]"
"sharing_option_private_heading" : "محدود"
"notify_heading_anonymous_user" : "Awanama"
"sharing_option_private_heading" : "Apribota"
"desc_password" : "□□□□"
"notify_heading_anonymous_user" : "گمنام"
"notify_heading_anonymous_user" : "Anonymní"
"desc_password" : "parooliväli"

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "Անանուն"
"sharing_option_private_heading" : "Kuvinjelwe"
"sharing_option_private_heading" : "□□□□"
"notify_heading_anonymous_user" : "Anonimo"
"notify_heading_anonymous_user" : "■■■■■■■■■"
"sharing_option_private_heading" : "■■■■■■■■■■"
"sharing_option_private_heading" : "Piiratud"
"google_api_key" : "AIzaSyBCcTM_PYMJ688Njw7NxBTh2DutdYNROrQ"
"sharing_option_private_heading" : "Dibatasi"
"notify_heading_anonymous_user" : "■■■■■■"
"sharing_option_private_heading" : "■■■■"
"sharing_option_private_heading" : "Begränsad"
"desc_password" : "□□□□"
"notify_heading_anonymous_user" : "Anonīms"
"getting_authentication_information" : "ກຳລັງເປີດເອກະສານ"

POSSIBLE SECRETS
"notify_heading_anonymous_user" : "■■■■■■"

PLAYSTORE INFORMATION

Title: Google Drive

Score: 4.3344564 **Installs:** 10,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Productivity **Play Store URL:** com.google.android.apps.docs

Developer Details: Google LLC, 5700313618786177705, 1600 Amphitheatre Parkway, Mountain View 94043, https://support.google.com/drive/?p=android_drive_help, apps-help@google.com,

Release Date: Apr 27, 2011 **Privacy Policy:** Privacy link

Description:

Google Drive, part of Google Workspace, is a safe place to back up and access all your files from any device. Easily invite others to view, edit, or leave comments on any of your files or folders. With Drive, you can: • Safely store and access your files anywhere • Quickly access recent and important files • Search for files by name and content • Share and set permissions for files and folders • View your content on the go while offline • Receive notifications about important activity on your files • Use your device's camera to scan paper documents Google Workspace subscribers have access to additional Drive functionality, including: • Easily managing users and file sharing to help meet data compliance needs • Sharing files and folders directly with groups or teams within your organization • Creating a shared drive to store all of your team's content Learn more about Google Workspace Drive: https://workspace.google.com/products/drive/ Learn more about Google Apps update policy: https://support.google.com/a/answer/6288871 Google accounts get 15GB of storage, shared across Google Drive, Gmail, and Google Photos. For additional storage, you can upgrade to Google Workspace or Google One as an in-app purchase. Subscriptions start at $1.99/month for 100 GB in the US, and can vary by region. Google Privacy Policy: https://www.google.com/intl/en_US/policies/privacy Google Drive Terms of Service: https://www.google.com/drive/terms-of-service Follow us for more: Twitter: https://twitter.com/googleworkspace Linkedin: https://www.linkedin.com/showcase/googleworkspace Facebook: https://www.facebook.com/googleworkspace/
