MOBSF

ANDROID STATIC ANALYSIS REPORT

Settings (3.0.1)

File Name:	AnyControl.apk
Package Name:	com.android.service.setting
Scan Date:	Aug. 1, 2024, 10:48 p.m.

App Security Score: 49/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	65	2	2	1

FILE INFORMATION

File Name: AnyControl.apk
Size: 16.77MB

MD5: 8e11b5ca240cc56f7118b8e3e3490b9f
SHA1: b5cbcce846f839133872b3d6cc1e0666b36d8011
SHA256: 6b17ee3410868902a4b9313b3ee854c03d5c2a62e2e92e367525adcfe2993b2a

APP INFORMATION

App Name: Settings
Package Name: com.android.service.setting
Main Activity: com.app.parentalcontrol.Activity.SplashScreen
Target SDK: 23
Min SDK: 19
Max SDK:
Android Version Name: 3.0.1
Android Version Code: 301

APP COMPONENTS

Activities: 39
Services: 20
Receivers: 15
Providers: 3
Exported Activities: 4
Exported Services: 11
Exported Receivers: 11
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: CN=StaffControl, OU=EmpolyeeMonitoring, O=ParentalControl, L=StaffControl, ST=EmpolyeeMonitoring, C=ParentalControl
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-04-24 04:40:07+00:00
Valid To: 2048-04-17 04:40:07+00:00
Issuer: CN=StaffControl, OU=EmpolyeeMonitoring, O=ParentalControl, L=StaffControl, ST=EmpolyeeMonitoring, C=ParentalControl
Serial Number: 0x1
Hash Algorithm: sha256
md5: 39dfc4da0af619e6836941a13714a6f7
sha1: 8c4e58eab4d86aac8f4f32dd9b9a29726866b226
sha256: 03f9574c551050f6e34621575339d49e170cffaf39f92d7ea62cc0dbd3ed5774
sha512: df487bde3011e5843d9fc8d8b2715a6f141b23ca07e9f2f629021bd76a8153f299de6126fb681c5ad3c3e739a96a7dfdd18d969fa19289638891222e0de8c0ee
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 266cb7437cb278fa558b96e48c250194854fd0a4569af2dcf53b7f969f1af1ba
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.REBOOT	SignatureOrSystem	force phone reboot	Allows the application to force the phone to reboot.
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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.WRITE_LOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
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.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_USER_DICTIONARY	dangerous	read user-defined dictionary	Allows an application to read any private words, names and phrases that the user may have stored in the user dictionary.
android.permission.WRITE_USER_DICTIONARY	normal	write to user-defined dictionary	Allows an application to write new words into the user dictionary.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERACT_ACROSS_USERS_FULL	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.WRITE_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
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.
android.permission.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAPTURE_AUDIO_OUTPUT	SignatureOrSystem	allows capturing of audio output.	Allows an application to capture audio output.
android.permission.POST_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check possible VM check
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	dexlib 2.x

classes.dex

FILE	DETAILS
classes2.dex	FINDINGS: Compiler — DETAILS: dexlib 2.x

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.app.parentalcontrol.Activity.TrialPage	Schemes: smartkey://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | 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.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 53 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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.
3	Service (com.app.parentalcontrol.Activity.floating_wizard_view.FloatingBall_Wizard) 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.
4	Service (com.app.parentalcontrol.Activity.floating_wizard_view.FloatingActivity_Service) 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.
5	Service (com.app.parentalcontrol.logging.ShowFloatWdnService) 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.
6	Broadcast Receiver (com.app.parentalcontrol.logging.Get10ClpInfoReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (.MyDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_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.
8	Launch Mode of activity (com.app.parentalcontrol.Activity.FloatActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
9	Launch Mode of activity (com.app.parentalcontrol.Activity.SplashScreen) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Launch Mode of activity (com.app.parentalcontrol.Activity.Home) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
11	Launch Mode of activity (com.app.parentalcontrol.Activity.Logging) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Launch Mode of activity (com.app.parentalcontrol.Activity.ImagePagerActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Launch Mode of activity (com.app.parentalcontrol.Activity.KeyloggingOption) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
14	Launch Mode of activity (com.app.parentalcontrol.Activity.timelimit.WarningBlockedActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
15	Launch Mode of activity (com.app.parentalcontrol.Activity.AppSecurityActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
16	Launch Mode of activity (com.app.parentalcontrol.Activity.ChangePin) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
17	Launch Mode of activity (com.app.parentalcontrol.Activity.LanguageActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
18	Launch Mode of activity (com.app.parentalcontrol.Activity.ChangePassword) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
19	Launch Mode of activity (com.app.parentalcontrol.Activity.LoginPage) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
20	Launch Mode of activity (com.app.parentalcontrol.Activity.TrialPage) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
21	Activity (com.app.parentalcontrol.Activity.TrialPage) 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.
22	Launch Mode of activity (com.app.parentalcontrol.Activity.ResetPasswordActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
23	Launch Mode of activity (com.app.parentalcontrol.Activity.ImageGridActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
24	Activity (com.android.inputmethod.latin.settings.SettingsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Activity (com.android.inputmethod.latin.spellcheck.SpellCheckerSettingsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
26	Activity (com.android.inputmethod.dictionarypack.DictionarySettingsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
27	Launch Mode of activity (com.app.parentalcontrol.Activity.SettingsActivityNew) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
28	Launch Mode of activity (com.app.parentalcontrol.root.PermissionsActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
29	Launch Mode of activity (com.app.parentalcontrol.Activity.DebugActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
30	Broadcast Receiver (com.app.parentalcontrol.logging.BkgroundWork) 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.
31	Broadcast Receiver (com.app.parentalcontrol.logging.StartupReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
32	Broadcast Receiver (com.app.parentalcontrol.logging.OutgoingCallObserver) 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.app.parentalcontrol.logging.screenshot.ScreenShotsReceiver) 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.app.parentalcontrol.logging.LicenseReceiver) 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.app.parentalcontrol.logging.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.
36	Broadcast Receiver (com.app.parentalcontrol.logging.GpsHandler) 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
37	Broadcast Receiver (com.app.parentalcontrol.logging.Receivers.NetworkChangeReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
38	Broadcast Receiver (com.android.inputmethod.dictionarypack.EventHandler) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
39	Service (com.app.parentalcontrol.logging.BackService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
40	Service (com.app.parentalcontrol.logging.iKClipboardService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
41	Service (com.app.parentalcontrol.logging.CallingRecordService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
42	Service (com.android.internet.Stenographer_Service) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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.
43	Service (com.android.inputmethod.latin.LatinIME) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_INPUT_METHOD [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.
44	Service (com.android.inputmethod.latin.spellcheck.AndroidSpellCheckerService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_TEXT_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.
45	Service (com.app.parentalcontrol.logging.LocationUpdatesService) 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
46	Service (com.app.parentalcontrol.logging.MyNotificationListenService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
47	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
48	High Intent Priority (2147483605) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
49	High Intent Priority (2147483645) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
50	High Intent Priority (2147483644) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
51	High Intent Priority (2147483643) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
52	High Intent Priority (2147483642) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
53	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
54	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
55	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/d.java a1/f.java a1/i.java b/a.java b/b.java b/c.java b0/b.java b0/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b0/l.java f0/j.java c0/e.java c1/a.java com/app/parentalcontrol/Activity/AppSecurityActivity.java com/app/parentalcontrol/Activity/ChangePassword.java com/app/parentalcontrol/Activity/ChangePin.java com/app/parentalcontrol/Activity/ClientShowLogs.java com/app/parentalcontrol/Activity/Home.java com/app/parentalcontrol/Activity/ImageGridActivity.java com/app/parentalcontrol/Activity/KeyloggingOption.java com/app/parentalcontrol/Activity/Logging.java com/app/parentalcontrol/Activity/LoginPage.java com/app/parentalcontrol/Activity/ResetPasswordActivity.java com/app/parentalcontrol/Activity/SettingsActivityNew.java com/app/parentalcontrol/Activity/SplashScreen.java com/app/parentalcontrol/Activity/TrialPage.java com/app/parentalcontrol/Activity/Wizard/Wizard0_Over_Protect_Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard1_Battery_Opt_Saver_Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard2_UsageAccess_Accessibility.java com/app/parentalcontrol/Activity/Wizard/Wizard3_NoRoot_ScreenShot_Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard4_StatusBar_HomeScreenIcon_Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard5_Settings_State_Activity_v3.java com/app/parentalcontrol/Activity/Wizard/Wizard6_Completed_Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard_Agreement_Web5Activity.java com/app/parentalcontrol/Activity/Wizard/Wizard_Agreement_WebActivity.java com/app/parentalcontrol/Activity/Wizard/Wizard_StatusBar_HomeSc_Activity.java com/app/parentalcontrol/Activity/Wizard/web_guide_expand_info/Singl_expand_list_Activity.java com/app/parentalcontrol/Activity/floating_wizard_view/BannerView_W.java com/app/parentalcontrol/Activity/floating_wizard_view/FloatingActivity_Service.java com/app/parentalcontrol/Activity/floating_wizard_view/FloatingBall_Wizard.java com/app/parentalcontrol/Activity/timelimit/AppLimitService.java com/app/parentalcontrol/Activity/timelimit/SettingGuide.java com/app/parentalcontrol/Camera/Camera2Service.java com/app/parentalcontrol/logging/BackService.java com/app/parentalcontrol/logging/CallingRecordService.java com/app/parentalcontrol/logging/CaptureService.java com/app/parentalcontrol/logging/Get10ClpInfoReceiver.java com/app/parentalcontrol/logging/GpsHandler.java com/app/parentalcontrol/logging/LicenseReceiver.java com/app/parentalcontrol/logging/MyApplication.java com/app/parentalcontrol/logging/MyNotificationListenService.java com/app/parentalcontrol/logging/Receivers/NetworkChangeReceiver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/app/parentalcontrol/logging/StartupReceiver.java com/app/parentalcontrol/logging/iKClipboardService.java com/app/parentalcontrol/root/PermissionsActivity.java com/bumptech/glide/b.java com/jssrc/resample/JSSRCResampler.java d/f.java d0/h.java d0/i.java d0/k.java d0/q.java d0/z.java d1/a.java d1/c.java d1/e.java d1/g.java d1/h.java e0/i.java e0/j.java f0/e.java f0/i.java f1/e.java g0/a.java g3/a.java g3/b.java g3/c.java h/a.java h/b.java h/c.java h/d.java h0/c.java h0/d.java h0/f.java h0/s.java h0/t.java h2/b.java h4/i.java i/a.java i/b.java i1/g.java i1/o.java i2/c.java i4/a.java j0/a.java k/a.java k/b.java k/e.java k/h.java k/i.java k/j.java k/k.java k/l.java k/m.java k/q.java k/r.java k/s.java k/t.java k/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k0/b0.java k0/c.java k0/d.java k0/k.java k0/m.java k0/n.java k0/r.java k0/z.java l/b.java l/c.java l/d.java l/f.java l/g.java l/h.java l/i.java l/j.java l/k.java l/m.java l/q.java l1/f.java m/a.java m/c.java m/d.java m/e.java m/f.java m/g.java m/h.java m/i.java m/j.java m/k.java m/l.java m/m.java m/n.java m/o.java m/p.java n/a.java n/b.java n/c.java n/d.java n/e.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteCursor.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java o0/a.java o0/d.java o0/j.java o1/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p/a.java p/d.java q0/e.java q0/f.java q0/k.java q0/l.java q0/n.java q0/o.java r/c.java r/e.java r/f.java r/j.java r0/d.java t/a.java t0/h.java u/a.java u/b.java u0/i.java u3/b.java v/b.java v/c.java v/d.java w/a.java w/b.java w/c.java w/d.java w/g.java w/h.java w/i.java w/j.java w/k.java w/l.java w/m.java x/a.java x/b.java x/c.java x/d.java y0/a.java z/d.java z/e.java z0/b.java z0/f.java z0/g.java z0/h.java z0/i.java z0/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	a0/g.java b/a.java com/app/parentalcontrol/Activity/FloatActivity.java d0/d.java d0/p.java d0/x.java l/q.java q1/e.java w/a.java x/b.java x/d.java
3	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/app/parentalcontrol/Activity/ClientShowLogs.java
4	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	d1/a.java k/t.java v/c.java w/a.java w/b.java w/c.java w/d.java w/g.java w/h.java w/l.java w/m.java x/d.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	a1/i.java b3/e.java com/app/parentalcontrol/Activity/TrialPage.java com/app/parentalcontrol/logging/MyApplication.java d/b.java d/f.java d1/g.java k/s.java l/g.java z0/g.java
6	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/app/parentalcontrol/Activity/SettingsActivityNew.java k/j.java
7	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	h2/c.java
8	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/app/parentalcontrol/logging/iKClipboardService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	e4/a.java e4/d.java i4/a.java v3/u.java
10	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	k/n.java x/c.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	w3/c.java
12	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	h2/b.java
13	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	k/h.java k/t.java
14	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	o1/h.java
15	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	k/h.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libresrtmp.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: ['__strchr_chk', '__strrchr_chk', '__vsprintf_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libwebpModule.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: ['__memcpy_chk']	False warning Symbols are available.
3	armeabi-v7a/librestreaming.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.
4	armeabi-v7a/libshout-jni.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.
5	armeabi-v7a/liblamejni.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	armeabi-v7a/libshout.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: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk']	False warning Symbols are available.
7	armeabi-v7a/liblame.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.
8	armeabi-v7a/libvorbis-jni.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.
9	armeabi-v7a/liblamemp3.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: ['__vsnprintf_chk', '__vsprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libjni_latinime.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.
11	armeabi-v7a/libsqlcipher.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.
12	armeabi-v7a/libogg.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.
13	armeabi-v7a/libvorbis.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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libresrtmp.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: ['__strchr_chk', '__strrchr_chk', '__vsprintf_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
15	armeabi-v7a/libwebpModule.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: ['__memcpy_chk']	False warning Symbols are available.
16	armeabi-v7a/librestreaming.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.
17	armeabi-v7a/libshout-jni.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
18	armeabi-v7a/liblamejni.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.
19	armeabi-v7a/libshout.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: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk']	False warning Symbols are available.
20	armeabi-v7a/liblame.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.
21	armeabi-v7a/libvorbis-jni.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
22	armeabi-v7a/liblamemp3.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: ['__vsnprintf_chk', '__vsprintf_chk']	False warning Symbols are available.
23	armeabi-v7a/libjni_latinime.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.
24	armeabi-v7a/libsqlcipher.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.
25	armeabi-v7a/libogg.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
26	armeabi-v7a/libvorbis.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']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	20/24	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.GET_ACCOUNTS, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK
Other Common Permissions	12/45	android.permission.PACKAGE_USAGE_STATS, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.READ_CALENDAR, android.permission.MODIFY_AUDIO_SETTINGS, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WRITE_CONTACTS, android.permission.FLASHLIGHT, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api3.anycontrol.org	ok	**IP:** 188.114.97.10 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
remotecontrol-2e3b4.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
imo.im	ok	**IP:** 83.229.97.15 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Borehamwood **Latitude:** 51.654678 **Longitude:** -0.277620 **View:** Google Map
www.icecast.org	ok	**IP:** 140.211.166.31 **Country:** United States of America **Region:** Oregon **City:** Eugene **Latitude:** 44.036083 **Longitude:** -123.052429 **View:** Google Map
my.اني	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
anycontrol.app	ok	**IP:** 172.67.207.131 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.251.37.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
co4-client-s.gateway.messenger.live.com	ok	**IP:** 13.83.65.43 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
lame.sf.net	ok	**IP:** 104.18.20.237 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.mp3dev.org	ok	**IP:** 142.251.36.243 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
my.anycontrol.app	ok	**IP:** 172.67.207.131 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://remotecontrol-2e3b4.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
g@groups.kik	w/d.java

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Подразумевано"
"key_preview_popup_dismiss_delay" : "ไลยะเวลาการสะแดงโตอัตสอบ"
"key_preview_popup_dismiss_default_delay" : "Lehenetsia"
"enter_userName" : "□□□□□"

POSSIBLE SECRETS
"firebase_database_url" : "https://remotecontrol-2e3b4.firebaseio.com"
"key_preview_popup_dismiss_default_delay" : "Predeterminada"
"key_preview_popup_dismiss_no_delay" : "■■■■□■■□"
"key_preview_popup_dismiss_default_delay" : "Oletus"
"show_language_switch_key" : "ปุ่มป่฽บผาสๆ"
"key_preview_popup_dismiss_default_delay" : "Numatytasis"
"key_preview_popup_dismiss_default_delay" : "Padrão"
"show_language_switch_key" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "ล่าเลิ่มต้ั้บ"
"key_preview_popup_dismiss_delay" : "Sleutelopspringer-wagperiode"
"key_preview_popup_dismiss_default_delay" : "□□"
"key_preview_popup_dismiss_delay" : "□□□□□□□□"
"key_preview_popup_dismiss_delay" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Әдепкі"
"key_preview_popup_dismiss_default_delay" : "Default"
"key_preview_popup_dismiss_default_delay" : "تلقائي"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■"
"Reg_EnterLicKey" : "□□□□□□□□"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□□□□□"
"key_preview_popup_dismiss_no_delay" : "■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Default"

POSSIBLE SECRETS
"key_preview_popup_dismiss_default_delay" : "Sjálfgefið"
"Debug_Licensekey" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Chaguomsingi"
"key_preview_popup_dismiss_default_delay" : "ڈیفالٹ"
"Lic_key_not_exist" : "□□□□□□□□"
"prefs_key_longpress_timeout_settings" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Okuzenzakalelayo"
"key_preview_popup_dismiss_no_delay" : "Viivituseta"
"prefs_key_longpress_timeout_settings" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "□□□"
"key_preview_popup_dismiss_no_delay" : "Kechikishsiz"
"prefs_enable_emoji_alt_physical_key" : "■■■■■■■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_no_delay" : "Хүлээхгүй"
"key_preview_popup_dismiss_default_delay" : "■■■■□■■■■■■□■"
"key_preview_popup_dismiss_default_delay" : "Privzeto"
"key_preview_popup_dismiss_default_delay" : "ნაგულისხმევი"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Προεπιλογή"
"show_language_switch_key" : "■■■■■■■■■■■■■■■■■■■"
"show_language_switch_key" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■■■"

POSSIBLE SECRETS
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Стандардно"
"Lic_key_not_exist" : "[redacted]"
"Reg_EnterLicKey" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Varsayılan"
"key_preview_popup_dismiss_default_delay" : "Výchozí"
"key_preview_popup_dismiss_default_delay" : "Verstek"
"key_preview_popup_dismiss_default_delay" : "Үндсэн"
"key_preview_popup_dismiss_no_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Predeterminado"
"key_preview_popup_dismiss_default_delay" : "Vaikeseade"
"key_preview_popup_dismiss_no_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Prestabilit"
"show_language_switch_key_summary" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Predeterminat"
"key_preview_popup_dismiss_default_delay" : "Podrazumevano"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_delay" : "[redacted]"
"show_language_switch_key" : "Kielenvaihtonäppäin"
"google_api_key" : "AIzaSyBmVGJTy-DJoCOK-Nnl2u5ExfiElQq2AHc"
"key_preview_popup_dismiss_default_delay" : "[redacted]"

POSSIBLE SECRETS
"key_preview_popup_dismiss_delay" : "□□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Predefinito"
"google_crash_reporting_api_key" : "AIzaSyBmVGJTy-DJoCOK-Nnl2u5ExfiElQq2AHc"
"show_language_switch_key_summary" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Демейки"
"Reg_InCorrectLicKey" : "□□□□□□"
"key_preview_popup_dismiss_delay" : "Tasten-Pop-up"
"prefs_key_longpress_timeout_settings" : "□□□□□□"
"Debug_Licensekey" : "□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Zadano"
"key_preview_popup_dismiss_default_delay" : "Standart"
"key_preview_popup_dismiss_no_delay" : "■■■■■■■■■■■■■■■■■■"
"key_preview_popup_dismiss_no_delay" : "ข้ถ้อซ่วงเวลา"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■"
"key_preview_popup_dismiss_no_delay" : "Дapoo"
"prefs_key_longpress_timeout_settings" : "□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "□□"
"key_preview_popup_dismiss_no_delay" : "□□□"
"Reg_InCorrectLicKey" : "□□□□□□"
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□"
"show_language_switch_key" : "Taal-wisselsleutel"
"prefs_key_longpress_timeout_settings" : "□□□□□□□"

POSSIBLE SECRETS
"Debug_Licensekey" : "Lizenzschlüssel"
"show_language_switch_key" : "[redacted]"
"enter_userName" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Noklusējums"
"prefs_enable_emoji_alt_physical_key" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Standard"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "Նախնականը"
"key_preview_popup_dismiss_default_delay" : "پیش‌فرض"
"key_preview_popup_dismiss_default_delay" : "Standaard"
"com.google.firebase.crashlytics.mapping_file_id" : "927164503f4e4e918253207d61e42c25"
"key_preview_popup_dismiss_default_delay" : "Predvolené"
"key_preview_popup_dismiss_default_delay" : "Lalai"
"key_preview_popup_dismiss_default_delay" : "Predefinido"
"key_preview_popup_dismiss_default_delay" : "Alapbeállítás"
"show_language_switch_key_summary" : "[redacted]"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"prefs_enable_emoji_alt_physical_key" : "[redacted]"
"show_language_switch_key" : "Sprachwechsel"
"enter_userName" : "Entr.NomUtilis"

POSSIBLE SECRETS
"show_language_switch_key_summary" : "ສະແດງໃນເວລາທີ່ຕ້ວເລືອກການປ້ອນຂ້ມູນຫຼາຍໂຕຖືກເປີດຢູ່"
"prefs_key_longpress_timeout_settings" : "ໄລຍະເວລາຂອງການກົດປຸ່ມ"
ccc707d2924768f2cc12bc8b
470fa2b4ae81cd56ecbcda9735803434cec591fa
258EAFA5-E914-47DA-95CA-C5AB0DC85B11