ANDROID STATIC ANALYSIS REPORT

Castlight (12.11.0)

File Name: com.castlight.clh.view_40601.apk

Package Name:	com.castlight.clh.view
Scan Date:	Aug. 29, 2025, 9:07 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	16	3	3	1

FILE INFORMATION

File Name: com.castlight.clh.view_40601.apk
Size: 85.24MB
MD5: 77bcc2b67f9b6aa3093b9018c5fbad13
SHA1: bf5194e236df5eb9fc996f3bd0c555aacddeb6aa
SHA256: 8f1c6e810fbce5bbe014ac10e6f88971762662ace35aa171bbf2872ac1ee4d8a

APP INFORMATION

App Name: Castlight
Package Name: com.castlight.clh.view
Main Activity: com.castlight.clh.view.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 12.11.0
Android Version Code: 40601

APP COMPONENTS

Activities: 12
Services: 10
Receivers: 8
Providers: 6
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: ST=US, L=SF, O=Castlighthealth, CN=Castlighthealth
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-11-02 09:57:53+00:00
Valid To: 2061-10-20 09:57:53+00:00
Issuer: ST=US, L=SF, O=Castlighthealth, CN=Castlighthealth
Serial Number: 0x4eb11421
Hash Algorithm: sha1
md5: 6f46d5ab68747e3e2fbd62e1ef89c03c
sha1: 299734bee6737f822a348f9042890822de27ce5e
sha256: cecb264eaafd96f3650b1808f0e1268d5da3b6413b1a4281e1dc0055a07eab68
sha512: d805be0a408a8fd8a3c1fc562bca1d73a1ee9c507e5c1a44e2c01ea58ca1c01973961828c69994e161e2a7dc6f2eb778d116776802f834b32c7057a6bee1d034
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: af03ad71df5651faebeb7a09371a1cabb56460f6a452597e2b82cffd76ed8f50
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

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.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.BODY_SENSORS	dangerous	grants access to body sensors, such as heart rate.	Allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.castlight.clh.view.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>77bcc2b67f9b6aa3093b9018c5fbad13.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Protector</td><td>FreeRASP</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.castlight.clh.view.MainActivity	Schemes: Castlight://, castlight://, https://, Hosts: click.secure.castlighthealth.com, m.us.castlighthealth.com, m.denpreprod.castlighthealth.com, m.gcp-int.castlighthealth.com, m.gcp-qa.castlighthealth.com, us.castlighthealth.com, denpreprod.castlighthealth.com, gcp-int.castlighthealth.com, gcp-qa.castlighthealth.com, m.gcp-preprod.castlighthealth.com, m.gcp-prod.castlighthealth.com, gcp-preprod.castlighthealth.com, gcp-prod.castlighthealth.com, Path Prefixes: /redirect.html, /?redirect_token, /oidc_redirect.html, /oidc_login_initiation.html,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **1** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (com.castlight.clh.view.plugins.VideoPlayerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.castlight.clh.view.plugins.amwell.util.CSVisitFinishedActivity) 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.
4	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) 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.
5	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.
6	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.
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

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	a0/d.java a3/f0.java a3/g0.java a3/h0.java a5/f.java a5/h.java b4/a.java b5/f.java c4/a.java com/americanwell/sdk/internal/b/n.java com/salesforce/android/service/common/utilities/lifecycle/LifecycleEvaluator.java com/salesforce/android/service/common/utilities/lifecycle/LifecycleMetricWatcher.java com/salesforce/android/service/common/utilities/lifecycle/LifecycleStateWatcher.java f3/d.java h3/a.java j3/f.java n2/d.java n2/i.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java p0/r.java r/c.java r9/b.java t/e.java uk/co/workingedge/phonegap/plugin/LaunchReview.java w0/h.java w2/a.java w2/b.java w2/h.java w2/i.java w2/j.java w2/k.java w2/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x/p0.java x2/f.java x2/h.java y0/c.java z2/g.java z2/h.java z3/f0.java
2	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	a0/n.java com/akamai/botman/h.java com/americanwell/sdk/internal/b/o.java e7/d.java h7/j.java i7/e.java q3/a.java r1/d1.java r1/z.java s1/a.java x8/a.java x8/b.java y8/a.java z3/x2.java
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	z3/x2.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a5/h.java
5	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	com/capacitorjs/plugins/camera/CameraUtils.java com/getcapacitor/BridgeWebChromeClient.java v2/i.java w0/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/americanwell/sdk/entity/SDKErrorReason.java com/americanwell/sdk/entity/SDKSuggestion.java com/americanwell/sdk/internal/AWSDKImpl.java com/americanwell/sdk/manager/ValidationConstants.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationStorage.java com/capacitorjs/plugins/localnotifications/TimedNotificationPublisher.java com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/salesforce/android/chat/core/internal/filetransfer/FileUploadRequestComposer.java com/salesforce/android/service/common/liveagentclient/SessionInfo.java com/salesforce/android/service/common/liveagentclient/request/LiveAgentRequest.java o/a.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/capacitorjs/plugins/camera/CameraUtils.java com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java com/salesforce/android/chat/ui/internal/filetransfer/ImageContentResolver.java nl/xservices/plugins/SocialSharing.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/capacitorjs/plugins/clipboard/Clipboard.java nl/xservices/plugins/SocialSharing.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	b7/g.java com/americanwell/sdk/internal/b/k.java com/americanwell/sdk/internal/b/m.java com/americanwell/sdk/internal/b/n.java com/americanwell/sdk/internal/d/d/f.java n2/d.java n2/h.java n2/i.java o2/j.java o2/k.java z3/b0.java z3/e.java z3/g1.java z3/u2.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a2/c.java f3/b.java o6/b.java
11	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	com/akamai/botman/ac.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/americanwell/sdk/internal/util/APIUtil.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__vsnprintf_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__vsnprintf_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi-v7a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi-v7a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__vsnprintf_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	arm64-v8a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	arm64-v8a/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	arm64-v8a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__vsnprintf_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86_64/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	x86_64/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86_64/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86_64/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	armeabi-v7a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	armeabi-v7a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	armeabi-v7a/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	armeabi-v7a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	x86/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	x86/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	x86/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_SET_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	x86/libtmlib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	x86/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	x86/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/americanwell/sdk/internal/d/e/b.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/capacitorjs/plugins/browser/Browser.java com/capacitorjs/plugins/browser/BrowserPlugin.java com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/LocalNotificationsPlugin.java com/castlight/clh/view/plugins/CallNumber.java com/castlight/clh/view/plugins/CapacitorVideoPlayer.java com/getcapacitor/Bridge.java com/phonegap/plugins/nativesettings/NativeSettings.java com/ryltsov/alex/plugins/file/opener/FileOpenerPlugin.java com/salesforce/android/chat/ui/internal/chatfeed/viewholder/ReceivedLinkPreviewMessageViewHolder.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java nl/xservices/plugins/Calendar.java uk/co/workingedge/LaunchNavigator.java uk/co/workingedge/phonegap/plugin/LaunchReview.java w2/f.java x2/f.java z3/w1.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/capacitorjs/plugins/browser/Browser.java com/castlight/clh/view/plugins/CallNumber.java nl/xservices/plugins/Calendar.java uk/co/workingedge/LaunchNavigator.java x2/f.java
00089	Connect to a URL and receive input stream from the server	command network	com/akamai/botman/b.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java n2/i.java p6/c.java z3/j0.java z3/v1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java z3/j0.java z3/v1.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java z3/j0.java z3/v1.java
00036	Get resource file from res/raw directory	reflection	com/capacitorjs/plugins/browser/Browser.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationChannelManager.java com/capacitorjs/plugins/pushnotifications/NotificationChannelManager.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java com/phonegap/plugins/nativesettings/NativeSettings.java uk/co/workingedge/phonegap/plugin/LaunchReview.java x2/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	c0/d.java com/americanwell/sdk/internal/b/o.java com/capacitorjs/plugins/filesystem/Filesystem.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/getcapacitor/AndroidProtocolHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java h3/a.java h7/i.java n2/j.java q5/b0.java t5/d.java v2/i.java w0/h.java
00022	Open a file from given absolute path of the file	file	com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/filesystem/Filesystem.java com/capacitorjs/plugins/filesystem/FilesystemPlugin.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java r1/a.java w0/h.java
00012	Read data and put it into a buffer stream	file	w0/h.java
00091	Retrieve data from broadcast	collection	com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/getcapacitor/Bridge.java r9/b.java
00109	Connect to a URL and get the response code	network command	com/akamai/botman/b.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java n2/i.java p6/c.java s2/c.java v2/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00034	Query the current data network type	collection network	com/americanwell/sdk/internal/util/b.java
00183	Get current camera parameters and change the setting.	camera	org/webrtc/Camera1Session.java
00112	Get the date of the calendar event	collection calendar	com/americanwell/sdk/entity/SDKLocalDate.java com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java nl/xservices/plugins/Calendar.java
00096	Connect to a URL and set request method	command network	com/akamai/botman/b.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java n2/i.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/filesystem/Filesystem.java v2/i.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/castlight/clh/view/plugins/amwell/services/SecureMessageService.java
00189	Get the content of a SMS message	sms	com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00009	Put data in cursor to JSON object	file	com/americanwell/sdk/internal/b/n.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java v2/i.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java v2/i.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00200	Query data from the contact list	collection contact	com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00187	Query a URI and check the result	collection sms calllog calendar	com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00201	Query data from the call log	collection calllog	com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java nl/xservices/plugins/Calendar.java nl/xservices/plugins/accessor/AbstractCalendarAccessor.java
00075	Get location of the device	collection location	com/capacitorjs/plugins/geolocation/Geolocation.java g/w.java

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	com/capacitorjs/plugins/camera/CameraPlugin.java
00202	Make a phone call	control	com/castlight/clh/view/plugins/CallNumber.java
00203	Put a phone number into an intent	control	com/castlight/clh/view/plugins/CallNumber.java
00014	Read file into a stream and put it into a JSON object	file	v2/i.java
00004	Get filename and put it to JSON object	file collection	v2/i.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	v2/i.java
00147	Get the time of current location	collection location	g/w.java
00115	Get last known location of the device	collection location	g/w.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java h6/c.java
00056	Modify voice volume	control	com/americanwell/sdk/internal/d/g/a.java org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java
00064	Monitor incoming call status	control	com/americanwell/sdk/internal/d/g/a.java
00102	Set the phone speaker on	command	com/americanwell/sdk/internal/d/g/a.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java
00162	Create InetSocketAddress object and connecting to it	socket	com/americanwell/sdk/internal/util/c.java
00163	Create new Socket and connecting to it	socket	com/americanwell/sdk/internal/util/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	com/salesforce/android/service/common/utilities/internal/android/notification/SalesforceNotificationManager.java
00192	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java
00153	Send binary data over HTTP	http	com/akamai/botman/b.java com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00045	Query the name of currently running application	collection reflection	com/americanwell/sdk/internal/b/n.java
00078	Get the network operator name	collection telephony	com/americanwell/sdk/internal/d/b/d.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://castlight-app.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/579430826825/namespaces/firebase:fetch?key=AIzaSyAHhv-qzDNIGePUU9JSr8kb6382V3fbBTc. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.GET_TASKS
Other Common Permissions	8/44	android.permission.BLUETOOTH, android.permission.CALL_PHONE, android.permission.READ_CALENDAR, android.permission.ACTIVITY_RECOGNITION, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS

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
apim.cformanalytics.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 74.125.138.155 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.whatsapp.com	ok	**IP:** 157.240.11.53 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
citymapper.com	ok	**IP:** 141.101.90.107 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
reports.crashlytics.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
share.here.com	ok	**IP:** 18.155.173.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
capacitorjs.com	ok	**IP:** 104.21.93.31 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
update.crashlytics.com	ok	**IP:** 142.251.15.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.tytocare.com	ok	**IP:** 40.112.243.63 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
app-measurement.com	ok	**IP:** 64.233.177.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 74.125.21.157 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
firebaseinstallations.googleapis.com	ok	**IP:** 142.251.15.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
hub.samsungapps.com	ok	**IP:** 34.240.53.86 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
maps.google.com	ok	**IP:** 173.194.219.139 **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.

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 173.194.219.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.webrtc.org	ok	**IP:** 64.233.176.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 142.250.9.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
castlight-app.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
webrtc.googlesource.com	ok	**IP:** 74.125.21.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
console.firebase.google.com	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 64.233.176.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomediacodec.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	x2/l.java
someone@domain.com	nl/xservices/plugins/SocialSharing.java
appro@openssl.org	lib/arm64-v8a/libjingle_peerconnection_so.so
ftp@example.com	lib/arm64-v8a/libclib.so
ftp@example.com	lib/x86_64/libclib.so
ftp@example.com	lib/armeabi-v7a/libclib.so
ftp@example.com	lib/x86/libclib.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so
ftp@example.com	apktool_out/lib/arm64-v8a/libclib.so
ftp@example.com	apktool_out/lib/x86_64/libclib.so

EMAIL	FILE
ftp@example.com	apktool_out/lib/armeabi-v7a/libclib.so
ftp@example.com	apktool_out/lib/x86/libclib.so

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
"awsdk_toggle_mic_txt" : "MIC"
"awsdk_tyto_setup_title" : "□□□□"
"awsdk_invite_guest_dialog_button_cancel" : "Annuler"
"awsdk_visit_camera_deactivated_wcag" : "Камеру"
"awsdk_invite_guest_list_email_order_third" : "Dritte"
"awsdk_visit_camera_activated_wcag" : "Kamera-ON"
"awsdk_visit_default_guest_display_name" : "Guest"

POSSIBLE SECRETS
"awsdk_invite_guest_dialog_button_send" : "□□"
"awsdk_toggle_camera_txt" : "Камеры"
"awsdk_invite_guest_list_email_order_fifth" : "Fünfte"
"awsdk_invite_guest_txt" : "□□□□"
"awsdk_invite_guest_dialog_button_send" : "■■■■■"
"chat_session_button_transfer_initiated" : "□□□□□□□□□□□□□□□□"
"awsdk_toggle_camera_txt" : "Kamera"
"awsdk_invite_guest_list_email_order_sixth" : "השישי"
"awsdk_invite_guest_list_email_order_sixth" : "шестой"
"awsdk_image_desc_drawer" : "■■■■"
"awsdk_invite_guest_list_email_order_eight" : "huitième"
"awsdk_visit_drawer_deactivated_wcag" : "□□□□□"
"awsdk_visit_invite_guest_navigation_close_wcag" : "Закрыть"
"awsdk_tyto_txt" : "□□"
"awsdk_console_extension_positive" : "כן"
"awsdk_next_button" : "nächster"
"awsdk_validation_email_duplicate" : "□□□□□□□□"
"awsdk_invite_guest_list_email_order_fifth" : "Fifth"

POSSIBLE SECRETS
"awsdk_invite_guest_list_email_order_fourth" : "□□"
"awsdk_console_extension_positive" : "■■■"
"awsdk_tyto_show_tag" : "הצג"
"awsdk_button_bar_end" : "End"
"awsdk_generic_retry" : "Повторить"
"awsdk_invite_guest_list_email_order_first" : "□□"
"chat_minimized_post_session" : "□□□□□□□□□□□□□□"
"awsdk_invite_guest_dialog_button_send" : "Send"
"awsdk_invite_guest_list_email_order_second" : "שניה"
"awsdk_switch_camera_txt" : "■■■■■"
"awsdk_visit_speaker_deactivated_wcag" : "□□□□□□"
"awsdk_visit_default_guest_display_name" : "□□"
"chat_dialog_end_session_title" : "□□□"
"awsdk_console_end" : "■■■"
"awsdk_visit_call_me" : "□□□□□"
"awsdk_custom_toast_invites_not_sent" : "□□□□□□□"
"awsdk_invite_guest_list_email_order_third" : "□□"
"awsdk_toggle_mic_txt" : "מיקרופון"

POSSIBLE SECRETS
"awsdk_invite_guest_list_email_order_sixth" : "Sechsten"
"awsdk_console_end" : "Ende"
"chat_session_ended_by_agent" : "□□□□□□□□□□□□□□□□□□□□□□□□"
"awsdk_guest_console_exit" : "Sortie"
"awsdk_console_extension_negative" : "לא"
"awsdk_visit_invite_guest_navigation_close_wcag" : "Fermer"
"awsdk_console_cancel_visit_positive" : "Oui"
"awsdk_console_cancel" : "Отмена"
"awsdk_invite_guest_list_email_order_third" : "третий"
"awsdk_tyto_txt" : "Tyto"
"awsdk_visit_invite_guest_limit_button_ok" : "□□"
"awsdk_tyto_show_tag" : "■■■■■■"
"awsdk_invite_guest_list_email_order_ninth" : "neuvième"
"awsdk_invite_guest_list_email_order_seventh" : "□□"
"chat_dialog_end_session_title" : "Închideți?"
"awsdk_visit_report_filename_prefix" : "VisitReport"
"fileprovider_authority" : "com.castlight.fileprovider"
"awsdk_toggle_mic_txt" : "Микрофон"

POSSIBLE SECRETS
"chat_dialog_end_session_title" : "□□□"
"awsdk_visit_invite_guest_navigation_close_wcag" : "Close"
"awsdk_invite_guest_list_email_order_seventh" : "Seventh"
"chat_dialog_end_session_positive" : "■■■■■■■■■■■■■"
"awsdk_image_desc_toggle_dock" : "□□□□"
"awsdk_image_desc_toggle_speaker" : "□□□□□"
"awsdk_invite_guest_list_email_order_fourth" : "Vierter"
"awsdk_guest_console_exit" : "□□"
"awsdk_visit_invite_guest_navigation_close_wcag" : "□□"
"awsdk_permissions_denied_button" : "□□□□"
"chat_dialog_end_session_positive" : "□□□□□□"
"awsdk_generic_retry" : "□□"
"awsdk_invite_guest_list_email_order_first" : "первый"
"awsdk_tyto_show_tag" : "□□"
"chat_dialog_end_session_positive" : "□□□□□□□□"
"awsdk_invite_guest_list_email_order_seventh" : "siebte"
"awsdk_invite_guest_dialog_button_cancel" : "Отмена"
"awsdk_invite_guest_list_email_order_tenth" : "העשירי"

POSSIBLE SECRETS
"awsdk_done_button" : "Fait"
"awsdk_refresh_trying_to_reconnect" : "□□□□□□□□□□□□□□□□"
"awsdk_invite_guest_list_email_order_eight" : "■■■■■/■■■"
"awsdk_invite_guest_dialog_button_send" : "Отправить"
"awsdk_console_extension_negative" : "N°"
"awsdk_image_desc_drawer" : "Ящик"
"awsdk_video_conference_cancel" : "Cancel"
"awsdk_visit_loading_member" : "□□□□□□□□□□□□□□□□"
"awsdk_tyto_continue_tag" : "Продолжать"
"awsdk_console_end" : "Конец"
"awsdk_visit_chat_console_title" : "Chat-Besuch"
"awsdk_tyto_ssid_tag" : "Ssid"
"awsdk_tyto_txt" : "Тито"
"awsdk_toggle_speaker_txt" : "■■■■■"
"awsdk_invite_guest_dialog_button_cancel" : "□□"
"chat_session_button_transfer_initiated" : "■■■■■■■■■■■■■■■■■■■■■■■■"
"awsdk_permissions_denied_button" : "Ende-Besuch"
"awsdk_image_desc_refresh_video" : "□□□□"

POSSIBLE SECRETS
"awsdk_guest_console_exit" : "Выход"
"chat_dialog_end_session_title" : "□□□□□□□?"
"awsdk_next_button" : "□□□"
"awsdk_generic_retry" : "Retry"
"awsdk_switch_camera_txt" : "Переключатель"
"awsdk_invite_guest_txt" : "Invite"
"awsdk_invite_guest_list_email_order_second" : "□□"
"awsdk_tyto_password_tag" : "Пароль"
"awsdk_tyto_continue_tag" : "המשך"
"awsdk_tyto_go_back" : "Zurück"
"awsdk_guest_console_exit" : "Exit"
"awsdk_tyto_continue_tag" : "□□"
"awsdk_invite_guest_list_email_order_fifth" : "□□"
"awsdk_invite_guest_list_invited_guest_email" : "□□□□□□□"
"awsdk_button_bar_end" : "Конец"
"awsdk_video_conference_cancel" : "בטל"
"awsdk_invite_guest_list_email_order_fourth" : "Fourth"
"awsdk_invite_guest_list_email_order_sixth" : "sixième"

POSSIBLE SECRETS
"awsdk_invite_guest_list_email_order_fifth" : "■■■■■■■"
"awsdk_invite_guest_list_email_order_fourth" : "quatrième"
"awsdk_video_conference_cancel" : "Отмена"
"chat_minimized_post_session" : "■■■■■■■■■■■■■■■■■■■■■"
"awsdk_invite_guest_list_email_order_ninth" : "девятый"
"awsdk_visit_not_charged" : "(□□□□□□□□□□)"
"chat_session_ended_by_agent" : "□□□□□□□□□□□□"
"awsdk_invite_guest_list_email_order_second" : "■■■■■"
"awsdk_lab_result_filename_prefix" : "LabOrderResult"
"awsdk_video_conference_cancel" : "Annuler"
"awsdk_visit_chat_console_title" : "□□□□"
"awsdk_visit_call_me" : "Appelle-moi"
"awsdk_image_desc_invite_guest" : "□□□□"
"awsdk_console_cancel_visit_positive" : "Yes"
"awsdk_button_bar_end" : "Fin"
"awsdk_console_cancel_visit_positive" : "Ja"
"awsdk_invite_guest_list_email_order_eight" : "השמיני"
"awsdk_console_extension_negative" : "Nein"

POSSIBLE SECRETS
"awsdk_console_cancel_visit_negative" : "לא"
"awsdk_tyto_password_tag" : "□□"
"awsdk_provider_image_content_description" : "Anbieterimage"
"awsdk_done_button" : "□"
"awsdk_visit_invite_guest_navigation_close_wcag" : "סגור"
"awsdk_tyto_password_tag" : "■■■■■■■"
"awsdk_toggle_camera_txt" : "Camera"
"awsdk_visit_chat_console_started" : "□□□□□□□□□□□□"
"awsdk_video_conference_leave" : "Отпуск"
"awsdk_guest_console_exit" : "■■■■"
"awsdk_console_cancel_visit_negative" : "N°"
"awsdk_video_conference_cancel" : "Abbrechen"
"awsdk_invite_guest_dialog_button_send" : "Envoyer"
"awsdk_visit_invite_guest_limit_button_ok" : "Bien"
"awsdk_image_desc_drawer" : "תפריט"
"awsdk_visit_chat_console_title" : "צ'אט"
"awsdk_console_extension_positive" : "□□"
"awsdk_console_title" : "Video-Besuch"

POSSIBLE SECRETS
"awsdk_generic_retry" : "Réessayer"
"awsdk_toggle_speaker_txt" : "Haut-parleur"
"awsdk_invite_guest_list_email_order_ninth" : "Ninth"
"awsdk_button_bar_end" : "□□"
"awsdk_console_end" : "End"
"chat_session_ended_by_agent" : "□□□□□□□□□□"
"awsdk_console_cancel_visit_negative" : "Nein"
"chat_end_session_content_description" : "□□□□□□□"
"awsdk_video_conference_leave" : "■■■■"
"awsdk_visit_default_guest_display_name" : "אורח"
"awsdk_invite_guest_list_email_order_first" : "■■■■"
"awsdk_switch_camera_txt" : "Switch"
"awsdk_done_button" : "■■■■"
"awsdk_done_button" : "Done"
"chat_minimized_post_session" : "□□□□□□□□"
"awsdk_invite_guest_list_email_order_fourth" : "■■■■"
"awsdktest_remote_service_url" : "https://localhost:1112"
"awsdk_invite_guest_list_email_order_tenth" : "десятый"

POSSIBLE SECRETS
"awsdk_validation_email_invalid" : "□□□□□□□□□□□□□□"
"awsdk_console_cancel" : "□□"
"awsdk_invite_guest_list_email_order_sixth" : "Sixth"
"awsdk_video_conference_begin" : "□□□□□□□□"
"awsdk_console_title" : "□□□□"
"awsdk_visit_setting_up_video" : "□□□□□□□□□□□□"
"awsdk_double_tap_to_zoom" : "□□□□"
"awsdk_tyto_txt" : "■■■■■"
"awsdk_visit_invite_guest_limit_button_ok" : "Okay"
"awsdk_console_extension_negative" : "Нет"
"awsdk_console_cancel_visit_positive" : "Да"
"awsdk_invite_guest_list_email_order_fifth" : "пятый"
"awsdk_tyto_show_tag" : "Montrer"
"awsdk_ending_visit_permissions_guest" : "%1$s"
"awsdk_invite_guest_list_email_order_second" : "Zweite"
"awsdk_visit_connecting" : "Подождите."
"awsdk_switch_camera_txt" : "החלף"
"awsdk_visit_disconnected_member" : "□□□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"awsdk_toggle_speaker_txt" : "Speaker"
"awsdk_invite_guest_list_email_order_sixth" : "■■■"
"awsdk_toggle_speaker_txt" : "□□□"
"awsdk_send_guest_invite" : "□□□□"
"awsdk_visit_other_camera_activated_wcag" : "□□□□□□"
"awsdk_console_extension_positive" : "Да"
"awsdk_visit_wrapping_up" : "□□□□□□□□□"
"awsdk_console_extension_positive" : "Oui"
"awsdk_visit_front_camera_activated_wcag" : "□□□□□□"
"awsdk_tyto_txt" : "TYTO"
"awsdk_invite_guest_list_email_order_third" : "troisième"
"awsdk_invite_guest_list_email_order_sixth" : "□□"
"awsdk_visit_refresh_video" : "□□□□"
"awsdk_invite_guest_list_email_order_third" : "שלישי"
"awsdk_tyto_go_back" : "Retour"
"awsdk_console_end" : "Fin"
"awsdk_visit_connecting" : "□□□□"
"awsdk_console_cancel" : "Annuler"

POSSIBLE SECRETS
"awsdk_button_bar_end" : "Ende"
"awsdk_console_cancel_visit_negative" : "Нет"
"awsdk_console_cancel" : "Cancel"
"awsdk_console_cancel_visit_negative" : "No"
"awsdk_guest_console_exit" : "Ausfahrt"
"awsdk_switch_camera_txt" : "Interrupteur"
"firebase_database_url" : "https://castlight-app.firebaseio.com"
"awsdk_invite_guest_list_email_order_seventh" : "שביעי"
"awsdk_tyto_live_stream_support_url" : "https://support.tytocare.com"
"awsdk_tyto_dialog_header" : "□□□□□□□□□"
"awsdk_done_button" : "fertig"
"awsdk_next_button" : "Next"
"awsdk_console_extension_negative" : "No"
"awsdk_invite_guest_list_email_order_fourth" : "הרביעי"
"awsdk_invite_guest_list_email_order_tenth" : "■■■■■"
"awsdk_invite_guest_list_email_order_fifth" : "cinquième"
"awsdk_generic_retry" : "Wiederholen"
"chat_dialog_end_session_title" : "الوداع؟"

POSSIBLE SECRETS
"awsdk_console_cancel" : "Abbrechen"
"awsdk_reload_txt" : "Reload"
"chat_dialog_end_session_title" : "[redacted]?"
"chat_session_button_transfer_initiated" : "[redacted]"
"awsdk_toggle_camera_txt" : "[redacted]"
"awsdk_console_extension_negative" : "[redacted]"
"awsdk_invite_guest_list_email_order_eight" : "Eighth"
"awsdk_console_end" : "[redacted]"
"awsdk_image_desc_drawer" : "[redacted]"
"awsdk_invite_guest_list_email_order_third" : "Third"
"awsdk_console_extension_positive" : "Yes"
"awsdk_invite_guest_list_email_order_tenth" : "Zehnte"
"awsdk_reload_txt" : "Перезагрузка"
"chat_minimized_post_session" : "[redacted]"
"chat_session_button_transfer_initiated" : "[redacted]"
"awsdk_switch_camera_txt" : "Schalter"
"awsdk_invite_guest_list_email_order_fourth" : "четвёртый"
"awsdk_invite_guest_list_email_order_seventh" : "[redacted]"

POSSIBLE SECRETS
"awsdk_reloading_wcag" : "□□□□□□□"
"awsdk_invite_guest_dialog_button_cancel" : "Abbrechen"
"awsdk_console_cancel_visit_negative" : "■■■■"
"awsdk_visit_provider_name" : "□□□"
"awsdk_invite_guest_list_max_number_of_guests_invited" : "□□□□□□□□□□□"
"awsdk_done_button" : "Договорились"
"awsdk_visit_camera_deactivated_wcag" : "□□□□"
"awsdk_tyto_status_visit_connection_failed" : "□□□□□□□□□□□□□□□□□□"
"awsdk_visit_camera_activated_wcag" : "□□□□"
"awsdk_guest_console_exit" : "יציאה"
"awsdk_visit_establish_connection" : "□□□□□□□□□□□□"
"awsdk_button_bar_end" : "■■■"
"awsdk_invite_guest_list_email_order_ninth" : "Neunte"
"awsdk_visit_provider_may_call" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"awsdk_tyto_password_tag" : "סיסמה"
"awsdk_invite_guest_list_email_order_eight" : "□□"
"awsdk_invite_guest_list_email_order_ninth" : "התשיעי"
"awsdk_toggle_speaker_txt" : "Спикер"

POSSIBLE SECRETS
"awsdk_tyto_show_tag" : "Zeigen"
"awsdk_invite_guest_list_email_order_third" : "■■■■■"
"awsdk_image_desc_drawer" : "Schublade"
"awsdk_video_consumer_connect_failed_info" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"awsdk_invite_guest_list_email_order_first" : "Ersten"
"awsdk_visit_invite_guest_limit_button_ok" : "Хорошо"
"awsdk_invite_guest_dialog_button_send" : "שלח"
"awsdk_next_button" : "הבא"
"awsdk_tyto_show_tag" : "show"
"awsdk_tyto_cancel_pairing_button" : "□□□□"
"awsdk_visit_invite_guest_limit_button_ok" : "OK"
"chat_end_session_content_description" : "□□□□□□□□□"
"awsdk_invite_guest_list_email_order_eight" : "восьмой"
"awsdk_visit_mic_activated_wcag" : "מיקרופון"
"awsdk_toggle_mic_txt" : "□□□"
"awsdk_tyto_go_back" : "□□"
"awsdk_visit_rear_camera_activated_wcag" : "□□□□□□□□"
"awsdk_invite_guest_list_email_order_tenth" : "□□"

POSSIBLE SECRETS
"awsdk_toggle_speaker_txt" : "Lautsprecher"
"awsdk_image_desc_toggle_mic" : "□□□□□"
"awsdk_visit_default_guest_display_name" : "Gast"
"awsdk_image_desc_toggle_dock" : "Dock-ein/aus"
"awsdk_done_button" : "אישור"
"awsdk_visit_drawer_activated_wcag" : "□□□□"
"awsdk_console_extension_positive" : "Ja"
"awsdk_next_button" : "Следующий"
"awsdk_tyto_live_stream_paired_headline" : "Tyto-Gerät"
"awsdk_invite_guest_list_email_order_tenth" : "dixième"
"awsdk_invite_guest_list_email_order_second" : "deuxième"
"awsdk_tyto_continue_tag" : "Continue"
"awsdk_invite_guest_dialog_button_send" : "Senden"
"awsdk_console_cancel" : "בטל"
"chat_dialog_end_session_title" : "Elköszön?"
"awsdk_end_visit_wcag" : "□□□□"
"awsdk_tyto_ssid_tag" : "ssid"
"awsdk_button_bar_end" : "סיים"

POSSIBLE SECRETS
"awsdk_video_conference_cancel" : "□□"
"awsdk_tyto_password_tag" : "Password"
"awsdk_invite_guest_list_email_order_first" : "First"
"awsdk_invite_guest_list_email_order_first" : "premier"
"awsdk_toggle_camera_txt" : "□□"
"awsdk_video_consumer_reconnect_failed_info" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"awsdk_switch_camera_txt" : "□□"
"awsdk_console_extension_negative" : "□"
"com.google.firebase.crashlytics.mapping_file_id" : "990f7057b7224ec08b1cbbe6477f8120"
"awsdk_invite_guest_dialog_button_cancel" : "בטח"
"awsdk_tyto_live_stream_paired_headline" : "□□□□"
"awsdk_image_desc_drawer" : "Drawer"
"awsdk_tyto_go_back" : "חזור"
"awsdk_invite_guest_dialog_button_cancel" : "Cancel"
"awsdk_toggle_camera_txt" : "מצלמה"
"awsdk_invite_guest_list_email_order_second" : "Second"
"awsdk_invite_guest_list_email_order_fifth" : "חמישית"
"awsdk_reload_wcag" : "□□□□□□"

POSSIBLE SECRETS
"chat_end_session_content_description" : "■■■■■■■■■■■■■■■■■■■■■■"
"awsdk_visit_default_guest_display_name" : "Гость"
"awsdk_video_conference_leave" : "סיים"
"awsdk_invite_guest_list_email_order_seventh" : "septième"
"awsdk_visit_provider_name" : "Поставщик"
"awsdk_next_button" : "prochain"
"awsdk_video_conference_leave" : "Verlassen"
"awsdk_toggle_speaker_txt" : "רמקול"
"awsdk_console_cancel_visit_negative" : "□"
"awsdk_toggle_bluetooth_txt" : "Bluetooth"
"awsdk_tyto_password_tag" : "Passwort"
"awsdk_visit_trouble_reconnecting" : "□□□□□□□□□□□□□□□□□□"
"awsdk_invite_guest_list_email_order_seventh" : "седьмой"
"awsdk_invite_guest_dialog_header" : "□□□□"
"awsdk_console_end" : "סיים"
"awsdk_custom_toast_invites_sent" : "□□□□□□"
"awsdk_toggle_mic_txt" : "Mic"
"awsdk_visit_invite_guest_limit_button_ok" : "אוקיי"

POSSIBLE SECRETS
"awsdk_invite_guest_list_email_order_ninth" : "■■■■■"
"chat_dialog_end_session_title" : "Αποχωρείτε;"
"awsdk_invite_guest_list_email_order_first" : "ראשון"
"awsdk_console_cancel_visit_positive" : "כן"
"chat_dialog_end_session_title" : "□□□□□□□□□?"
"awsdk_invite_guest_list_email_order_tenth" : "Tenth"
"google_api_key" : "AIzaSyAHhv-qzDNIGePUU9JSr8kb6382V3fbBTc"
"awsdk_visit_default_guest_display_name" : "Invités"
"awsdk_tyto_show_tag" : "Показать"
"awsdk_next_button" : "■■■■"
"awsdk_tyto_status_main_button_timeout" : "□□□□□"
"awsdk_console_cancel_visit_positive" : "■■■"
"awsdk_video_conference_leave" : "□□"
"awsdk_visit_provider_name" : "■■■■■■■"
"awsdk_invite_guest_list_guests_email" : "□□□□□□□"
"awsdk_video_conference_leave" : "Congé"
"awsdk_provider_image_content_description" : "□□□□□□"
"awsdk_console_cancel_visit_positive" : "□□"

POSSIBLE SECRETS
"chat_session_ended_by_agent" : "[redacted]"
"google_crash_reporting_api_key" : "AIzaSyAHhv-qzDNIGePUU9JSr8kb6382V3fbBTc"
"chat_dialog_end_session_positive" : "□□□□"
"awsdk_generic_retry" : "[redacted]"
"awsdk_invite_guest_list_email_order_second" : "секунда"
"awsdk_image_desc_drawer" : "Tiroir"
"awsdk_visit_default_guest_display_name" : "[redacted]"
"awsdk_video_conference_leave" : "Leave"
"awsdk_tyto_continue_tag" : "continuer"
"awsdk_image_desc_toggle_camera" : "□□□□"
"awsdk_invite_guest_list_email_order_eight" : "Achte"
"awsdk_tyto_go_back" : "Вернуться"
"chat_end_session_content_description" : "□□□□□□□□□□□□□□"
"awsdk_build_revision" : "4fa26af085cbcd2d9052c9ba9976ce856ea7fe27"
"awsdk_visit_mic_deactivated_wcag" : "□□□□□"
"awsdk_invite_guest_list_email_order_ninth" : "□□"
0FAC210B244F0D07B64EB6678F5BDA37B93A68F4B50553193A713989B8B6AF5544A9211064424D
00AE2B0865484205F605AD7A9913C025AE3B79ED

POSSIBLE SECRETS
44AD32146849311EF951BC
579F2539446D365DAE77BA4AB503DB359F0346D78D1B6E2F7B7E7B998FBDAD4978A705114C661318
47AD30257B43110FFC73BC608F5ADC32
43A72A1B624B340FEA56B07D92
48A72B166E48421FEB4CB775DC60C63EAE3B6EE1A04E
65BA3612790C0D09FB50AB609957932BB52670E5F4594518387D2E8AA2BDBA5B44A9301C2B4A1005F505B2778540C733AF2A
43A7295372490E06F752BC61D240C6
43A0211E60690F1FF444AD7D8E7ED232A8297DE3A05E520938
02E44E5D2B0C424AB807B477985AD218AF223EBAF6
49A62D09255F1409B653BB7D840B8571AE2A68F5A4
55A62B1B6D450103F949907C8F47D230B12E68E9BB4573033F662899
41A6200F64450644E840AB7F9540C035B22132D5876E7F2A035A0CB999838F326E9C
63A0211E60620307FD1FF97A9D40F539BC3B69F2B17F451F3E7D259B8FB2A91A0CE82D136D43584A
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD298868D2B6F9A10384F732328D176F9749556DF38
41A6200F64450644E840AB7F9540C035B22132C69B79652B185B1EB28F8C8E3E729E0D3E4E
50AD3610625F1103F74BAA

POSSIBLE SECRETS
308201e53082014ea00302010202044f54468b300d06092a864886f70d0101050500303731 0b3009060355040613025553311030 0e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d313230333035303435323237 5a170d343230323236303435323237 5a3037310b3009060355040613025553311030 0e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567 30819f300d06092a864886f70d010101050003818d0030818902818100 8a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c5990503279827 3462bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001300d06092a864886f70d01010505000381810005129922 68a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122
459D172B71473633D016B742947ADF0A892B49EA9C59443E3D5D79BEFBBFEF22199826135B6A
61A6200F6445064ACB6192329E46DA30A96F7AEFA60B58547C4B7DC8
648E703E7A5F5510FC5FE9609A52D00D91196FF9E04D6F033E4211AD80959A10699100
41A6200F64450644E840AB7F9540C035B22132D5876E7F2E035B06B99F819438
47AD300D7943124AEA4AF770935CC772AE2A70E9BA5E58
49BB170478580707C857B6629941C725983E69E1B87F4F
04BB310E7B450103F750AA538C43C0
61BD30156E421603FB649456
6BAD3D0E7F43100FB84AAB329756CA7CAD2E6EE1B958000539342589A7BFF3
47AD300D7943124AEA4AF770895ADF38F33C79ECBD455514
53BD26176E4F162BF451BC609252C735AB2A52E1B94E53
41A6200F64450644E840AB7F9540C035B22132C69B79652B185B1EB28F8C8E3E729E0D3E4E73262BCC648641A57DF0
42A12A1962420535E850BB7E9550EC37B836
75A6251F6749421EF705AB778841DA39AB2A3CEDA14754053A782EDCB8BABA1545BA3753

POSSIBLE SECRETS
49BB00187D490E05E840AB5F9357D619B32E7EECB14F
46AD25097E5E073EFD56AD7B9254FA32BE2678E5BA5F53
4EA4064A3E755152AD66BF5DB87A812BBE1A56D08D446C2A7D580CCFA997BF376CA72B
65B0341868580B04FF05BB7B9257D62EFD2D69F4F44C4F186A7A3E90A7F2FD5B
48A937306A4B0B19F376AD679E
41A6200F64450644E840AB7F9540C035B22132D5846F61380F4B1BBD88989C3C659B1B2A42782A25CD718647AF76E1039C0C48C99B65
43A729536A420618F74CBD3C8A56DD38B4217A
64AD321468492B0EFD4BAD7B9A5AD62EAE
69A62D09624D0E03E24CB775
53AD270879451613C844AD7194
618D1752486E2145D64A89739857DA32BA
43A7295360431719F04CB2768947C73DF33D73EDB94A4E0D2D7139D2A7BABE1E4EBB21
41A6200F64450647FA50B07E98
49A76A1A62580A1FFA0BAF649E01836AED6171E1B3425307
47A72B1A6749423AF15DBC7EDC01
43A729537F5F0C0DB64DB076995ECA3DAD3F70E9A75F
41B834346558070DEA4CAD6BBF5BD63FB60A6EF2BB59
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD283928F3F778916382B4A0B0FF441

POSSIBLE SECRETS
0FB836126803011AED4CB77493
69A6301879420306B84CAA6189569335B36F68E8B10B4B0933673F93B9B6FD1949A62018790C060FEC40BA6699579D
48BC300D78164D45AC46BC76CE01D03DED792AE4E04841582B237CCEFDB0E41A46AE2245681C5153B650AA3F9952C028F07E32E1A3580E0A25612598E5BAB24119FA704E24580306EB40BA4D905CD403B92A6ADFB545441E257D2FA3ADA1B81E7FBF36147F494D35FC4ABA2D8C5AC339B12672E5E95F4100397128A3A7BCBA2449A6201873
41A428127C490639EC4AAB778F
48A937357E4D150FF168B670955FD60FB83D6AE9B74E53
55A6291C7847311EEA4CB775
49BB173847450C1FE060B7749341D039B9
65B027187B580B05F605BD678E5ADD3BFD2070E4F45B52092C713999A5B0B80800BA2110645A0306B6
48A9372F64431603F64289739F58D23BB83C55EEA75F410026712F
59B13D0426612F47FC41FE46DB7BFB66B02226F3A705733F194718AF91
50A927166A4B0723F643B6
45BE1C29456E175CF2729B779742D00FBC7D5AED9B436509006409BDAFB4A41D50A4324A461F4D32CE52AA2F
759D0E443C140B05DE4CED7BA55FF40DBF1A4ED2B96A4E193F727CCDBCEA962918AA13
6EA42C2F5B61091CC850B25A8F4BC631E42C5EFAE4684F20076D1DABFCE19A3118F10D39676D
53AD281465591A3AEA4AA9778E47DA39AE
49A62D09255F1409B642B67E9855DA2FB56270EFB3484118
43A7295360450C0DF744A962D241DC33A9

POSSIBLE SECRETS
4CA7231A62420539EB49897B925DDA32BA
43A0211E60690F1FF444AD7D8E7EDC38B823
49A62D09255F1409B643B07E995EDC32
41A6200F64450644E840AB7F9540C035B22132C99A7F653E04511F
0FBB3D0E7F490F45FE57B87F9944DC2EB66044F0BB58450808662298ACB6F31141BA
7083072E3A7C030EFC4CB775
53AC2F226C430D0DF4408662945CDD39823724B6
50A927166A4B0724F948BC
49A62712795E0709EC75B8719752D439932E71E5
4DAD6A0A6E451102ED0BBC6A8C
0FBB3D0E7F490F45E047B07CD357D239B02072F3A1
41BA213F62420318F140AA428E56C039B33B
65AC16056D650B3BC2499E758474F524A91B73F3A31F631B3E6772B3A9A49F0D77A22C24405A281E
43A729536F49140BFC53B87C9F569D2EB22068E3B8444107
43A0211E60690F1FF444AD7D8E71C13DB32B
6AB820136A411B39C263E827C444D71E911F5AF28C1A6A1C247F03B1F3A3991577B2770F444D5A58
61800615627B3B26EB6F9C40B852F164AD085EE7A27B642F7F5C0AC9BCF8AD2D59BB3C284E630A5BFB57E12F
46BA2118794D111ADA49B871975FDA2FA91979F2A7424F02

POSSIBLE SECRETS
62A9205D6A5E051FF540B766DC5ADD7C973C73EE
0FBB3D0E7F490F45E047B07C
42A3140E7E79061DDD55BA20C546823B911D5EB8A65C66297D6601BD8C97892172FE02055D485510
6D89082A4A7E2735D16B9F5D
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
44A1203C65481005F1419076BF5BD232BA2A
13A20225664B3258F04CAD4AAF59E725941C7FD2A67E532D7D7700C499809E2D4BFA72
61E8361878431718FB40F9749D5ADF39B96F68EFF448410026342890A4A0B85500E8
49A76A1A62580A1FFA0BAF649E01836AED6171E1B342530764782288AE
42BD2D116F7F0706F14BAC6AAC41DC2CB83D68F9
51AD2908255F0444FE44B277A350D231B83D7D
68F902127B562528F5609255B802FF34B13B4ED6976659552C4D26B9AE819C017589343161
43A729537F440B18FC55B860884A9D2FA83F79F2A158451E
4EA72A184E421005F449BC76
0FBB3D0E7F490F45E047B07CD344DB35BE27
47AD2A1879450135E01DEF4DCA07
6D80333E694F555FF9779176AF54F66CA40D75C4
0FAC25096A030E05FB44B53D9E5ADD73

POSSIBLE SECRETS
14920D3F52552B05C073BF23A44BF71D930648E8871F6506272C07A9B1BAAF2F51
55A10012337B0913EA6EA846C5758669993679B8874819183F551296BDAB954C54A6364D
41BA213C7B47112BEE44B07E9D51DF39
0FBB3D0E7F490F45F955A93D
41A6200F64450644F756F741B97FDA32A837
65BA3612790C1502F149BC329452C034B4217BA0B04A540D64
41A6200F64450644E840AB7F9540C035B22132D2916A64331A5C04B28E8C8E2F619C01
4DA9280A6A5E073AF946B2739B56FD3DB02A5EECB5484B0023673F
308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a13135361 6d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531325a170d3338313130373132 323531325a3081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a13135361 6d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c 35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0 c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b 6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b308201 07301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310 b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f727 06f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d7375 6e672e636f6d820900d20995a79c0daad6300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100329601fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430 369ac51530f63aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a429 9db4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512dfb28d42c 855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c810158
67FB2707384E270CDD4E9E22BA6BF13A9B1A59B596695334185802CBA0A2AB19728E
74A1291858550C09B84CAA6189569D72F3

POSSIBLE SECRETS
308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b300906035504061302b52311430120603550408130b536f757468204b6f726561133011060355040713 1133011060355040713 0a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d313130363232313232353133 5a170d333831313037313232 3531335a3081a2310b300906035504061302b52311430120603550408130b536f757468204b6f726561133011060355040713 0a5375776f6e2043697479311c301a060355040a131353616d 73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642 e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e967 8ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e2 75155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e6200677 55e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30 820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a5308 1a2310b300906035504061302b52311430120603550408130b536f757468204b6f726561133011060355040713 0a5375776f6e2043697479311c301a060355040a131353616d73756e672043 36f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616 6d73756e672e636f6d820900e5eff0a8f66d92b3300c0603551d130405300301 01ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fb ad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2ca a2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf 24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a
0FBE21136F431045FA4CB7
43A0211E607F0B07CB40AB7B9D5F
41B834346F490C1EF143B0778E
6EA7170868442403FD49BD578E41DC2E
43A72A0979430E2FE040BA67885ADC328E3B7DF4B1
4FBA2353675F1205EB40BD3C9152DD3DBA2A6E
43A72953784F0C44EA4AB6669D5DD72EB23875F4BC4455183A77
49A62D09255F1409B654BC7F8957
48A937307E401603E849BC419554DD3DA93A6EE5A7
4FAA2208784F031EF14AB75B8F40C639AE

POSSIBLE SECRETS
0FBB3D0E7F490F45FA4CB73D
75A62F13645B0C4AEA40B871885ADC32FD3B65F0B105
6FA42245644B2F23AB64A15E8864C66A89792DE2936D57211C2C0AABAE9AB84B47BD124564412606
50BA2D0B6240070DFD4198719F56C02F
52A76A156A5E061DF957BC3C8A5AC128A82E70DFB04E56052971
68A937156E483D07F142AB738856D7
46A736106A584A1EF04CAA3EDC19D22EBA3C35
65B034186858070EB876B075925ADD3BFD0C79F2A042460529753F99EB9BBC0848AD375D6A5E074AF64AAD329856D535B32A78A0BD4500382B783899A890B21546A123
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD28F968B32638D641B62490E0E
48A9373A64430506FD68B670955FD60FB83D6AE9B74E53
49BB0B096A6F0718EC4CBF7B9F52C73990266FF3BD4547
0FBB3D0E7F490F45FA4CB73DD256CB28F2
42A72B0958490E03F650A1428E5CC339AF3B65
6BA12A1A79430D1EB644A979
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD29D968F2869870A5359692E2FD9769C329A5AD630B9
42AD25094E540709ED51B07D9260C73DA92A
43A66A1A6E49091EF94BBE3C8C41DA2ABC2C65F3A44A4309
49BB00186959050DFD579A7D925DD63FA92A78

POSSIBLE SECRETS
02E44E5D2B0C424AB807BF7B9254D62EAD3D75EEA07D134E7036
41A428127C49063AF34297739156C0
43A7295371440B1BED55B23C8E5CDC28F32870EFB64A4C
73A0250F6E48423AEA40BF778E56DD3FB83C3CEDB54C490F6A722290AEF3B5124EBC641E64590E0EF602AD329E56933FAF2A7DF4B14F000E33342D95A7B6AE0253BC2110
75A6251F6749421EF705AB778841DA39AB2A3CE3B15954052C7D289DBFB6FD1349BB301279554C
54A9280E6E4F2105F643B075
41A6200F64450644E840AB7F9540C035B22132C19768653F194B05B99F8492296B9717294A7827
44B12A1C66450129F74BBF7B9B65D62EAE2673EE
75A621057B49011EFD41F9649D5FC639E76F
16B93E444C5E2A5EA94991718E65D21684177BDABC6271042852798D8C90EF3468AE
42A4251E60400B19EC40BD5A9D40DB39AE
73BD34187959110FEA0BB86297
66A6020F4C43320BAA6EEF5C9063E32487277BCBE06755361E700796BDB1A90E19A223046343540F
689F1B1F6A4F090FFC7AB2778540C733AF2A
46A12A1A6E5E1218F14BAD44CF
41B82D306E580A05FC6BB87F997DDC28922D7AF5A74841182F70
43A729536359031DFD4CF77A8B5AD7
1EE82D0E2B420D1EB8769153D101866AFD3D79F0A64E530924602A88A2BCB35B4FAE640963494219F142B77B9254933FB83D68E9B242430D3E716B95A5F39F1A53AD724925

POSSIBLE SECRETS
0FBB3D0E7F490F45E047B07CD35EC6
48BF061C6847070ED340A0719452DA32
49BB160865420B04FF76AC428E5CD039AE3C79F3954854053C7D3F8586B2B31A47AD36
43A729536A411202F757B861D25BDA38B82265F2BB44540D2E723999AE
48A72B166E48421FEB4CB775DC6BC333AE2A78
43A729537C56070FEA4AB666A307816BE47E2FB1FA4A5007
73BD370D624F0B05ED5698628C7ADD3AB2676CE1B740410B2F5D259AA4EE
65B034186858070EC844BA799D54D612BC2279A0BD5800023F7827D2
49BB1C0D645F070ECE40AB61955CDD1DAB2E75ECB5494C09
11FD7148391D555FA811E0
49A637096A400E0BEC4CB67CAF5CC62EBE2A
49BB120D657E1704F64CB775
41AC26226E420308F440BD
49BB051969690C0BFA49BC76
41A430187942031EF153BC519941C714BC3C74E5A7
618B103444623D39CC648D57
74A1291858550C09DD57AB7D8E
52A76A166E5E0C0FF40BB87C9841DC35B92D73EFA005480D38703C9DB9B6

POSSIBLE SECRETS
65BA3612790C0D09FB50AB609957932BB52670E5F459450125622292ACF3B91A54A9641B79430F4AF340A061885CC139
4DA9280A6A5E073AF946B2739B56C0
63FF353E474B2413F166B5229342DE65E51A5DF18D
0FBB3D0E7F490F45EB41F66A9E5ADD73
53E62A1873582E03F640F13B
6BA12A1A647E0D05EC0BB86297
43A729536A420618F74CBD3C8A56DD38B4217BAEB6424C00237A2CD282BD9C0B508A2D1167450C0DCB40AB649550D6729E0055CE
45B0301879420306C74CBD
43A0211E60690F1FF444AD7D8E75DA32BA2A6EF0A6424E18
41B834346558070DEA4CAD6B
70A9370E6E48421FF656AC628C5CC128B82B3CEBB152531825662E
74A9280E6E4F3D2FE051BC609252DF
63A0211E60620307FD1FF97F9D5FC43DAF2A4CE1B740410B2F6767DCA2BDBB141AE8
43A0211E607C1005E840AB668577D63EA8287BE1B64745
49A62D09255F1409B641AC7F8C5FDC3BBE2E68
73BC3614654B201FF149BD778E1B9A72BC3F6CECAD03421923782F99B992BE0F49A72A5425580D39EC57B07C9B1B9A
4D8F701A49410F22AD10A3689D5AD00BE4215EC29712610B1B2606889A87A71C13FC07166D7A1138
78B82B0E6E484203EB05B871885AC539

POSSIBLE SECRETS
43A729537845060BB64BBC65975ADD3BAF2073F4BD4553182B782799B9B6BC0859
0FBB3D0E244A1145EB40B57B9246CB73B8217AEFA64845
54A73453684D0C13F140F7768E56D231B12E72E4FA4641022B732E8E
77F9222D6966120EAC57AC73AB6BF63A8E0055B6AC6270593A4C20B587A0991771BB2F24
48BC300D78164D45AC46BC76CE01D03DED792AE4E04841582B237CCEFDB0E41A46AE2245681C5153B650AA3F9952C028F07E32E1A3580E0A25612598E5BAB24119FA704E24580306EB40BA4D905CD403AD3D73E48B4A4E08387B229894B5AF1E4597330F62580745C741B671C343DA2CB82375EEB116540D26672E9F94BFB21C7FA12A196E54
41A6200F64450644E840AB7F9540C035B22132C89D6F653305420EAE8792842477810A39447B31
75A6251F6749421EF705AB778841DA39AB2A3CF3BD4C4E0D3E613999E5
53AD281465591A2FF643B6609F56DE39B33B5AE9B84E630324602E92BF
41A6200F64450644E840AB7F9540C035B22132D1816E7235155507B094839C386B89033858
45B00B1B32552F13F04F81708878C324EF2046D4E278411E02
41A6200F64450644F756F7418540C739B01F6EEFA44E5218237138
43A0211E607C1005E840AB668564DB35BE2755F39B454C15057A0E91BEBFBC0F4FBA
688A1B3344783D2CD7709756
43A7295360450C0DEA4AB666D258DA32BA3A6FE5A6
65BA3612790C1502F149BC32905CD238B4217BA0956073
0FBB201E6A5E0645EF4CB7769344C0739F3C68D3BC4A52092E522490AFB6AF
43A729536359031DFD4CF7738C43DE3DAF2479F4

POSSIBLE SECRETS
43A729536F49140BFC53B87C9F569D2EB22068E3B84441073A783E8F
52A76A1F7E450E0EB655AB7D9846D028
42A4251E60400B19EC40BD429D50D83DBA2A52E1B94E53
49BB020F62480339FD57AF778E7FDA2FA92A72E9BA4C
13F927183C1E045BFE10BF23CB56D73FE57F2EB9EC1A19097A722A9EF2E4E54843AB744D3C145A53FA1DEB70CD058B6DEC7625B1E513450A7E7279C9FEE6E948
49BB173847450C1FE060B7739E5FD638
74A9280E6E4F2003F641B07C9B
729B05524E6F2045C86E9A41CD63D238B92672E7
52A76A1B6A4F1605EA5CAD778F47
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
43A729536A44070BFC4CAD779F1DC73DB13C79E38B58450F3F662288B2FDAE1E43BD36147F554C0BE84CF7469D5FC039BE
49A637096A400E39F750AB7199
50A927166A4B0727F94BB87599419D3BB83B55EEA75F4100A894ED9DACB6901A4EA923187902252FCC7A9457A872EC189C1B5DA9
49A6321C67450639F142B7738846C13999267BE5A75F6C053960
43A729536F450F05F653B076995C9D30A82C77F9A44A540F227139
7489082E4E6F3D23D66396

POSSIBLE SECRETS
308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040 7130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040 b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d010901 1613616e64726f696440616e64726f69642e636f6d301e170d3038303431353232343035305a170d333530 3930313232343035305a308194310b300906035504061302555331133011060355040813 0a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307 416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613 616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d 00308201080282010100 9c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350ec535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010057255 1b8d93a1f73de0f6d469f86dad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc059617cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357
43A0211E60690F1FF444AD7D8E63C133B93A7FF4
48A9373B6E4D161FEA408D778F47DA32BA0B7DF4B5
4DA92A086D4D011EED57BC60
44A120366E55311EF757BC519452DD3BB8
45BD6A1E634D0B04FE4CAB77D240C62CB83D6FF5
4FBA235366490D1DFB44AD3C9957CB2CB23C79E4FA4641022B732E8E
53AD360B624F0744F941BB3C8E5CDC28

POSSIBLE SECRETS
308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d01010505003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e696131 16301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964 3122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303232393031333334365a170d3335303731373031333334365a308194310b30090603 55040613025553311330110603550408130a43616c69666f726e696131163014060355040 7130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355 040b1307416e64726f69643110300e06035504031307416e64726f6964312230200 6092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f 70d01010105000382010d00308201080282010100d6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64 b8e4fea2d3e656f1e267a81bbfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2c b3f284a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e247553311c46b9af 76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a381fc3081f9301d0603551d0e04160414485900563d272c46ae118605a47419ac09 ca8c113081c90603551d230481c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c6966 6f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130741 6e64726f6964312230200 6092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d010 1050500038201010 07aaf968ceb50c441055118d0daabaf015b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c2 04eb15311f455d824b656dbe4dc2240912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea560 3b2c540dbd7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430eea7c26a1 c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d
53AD281465591A2FF643B6609F56D70EB82970E5B75F
43A729536D431A58FB4ABD77D25EDE31
470fa2b4ae81cd56ecbcda9735803434cec591fa
53BD370D624F0B05ED5689778E5EDA2FAE2673EE
53BD370D624F0B05ED56907C8F47D230B12E68E9BB4573033F662899
43A7295365431102ED43B667D252DD38AF2075E4FA5855422F782288AE
6F86012D4779314AD916E923CC
48A93734655A0306F1418A7B9B5DD228A83D79C4BD4C451F3E5A2A88A2A5B8
43A0211E607A0D03FB409473955FFD29B02D79F2
44AD321468492003F641B07C9B

POSSIBLE SECRETS
49A62712795E0709EC75B8719752D439932E71E59A4A54053C71
54BC123054640618F942B67C
43A0211E60690F1FF444AD7D8E77D62AB42C79
41A6200F64450644E840AB7F9540C035B22132D38D787429074B0AB08E81892477810A39447B
49BB160865420B04FF76AC428E5CD039AE3C79F3875F411839592A92AAB4B809
46A92F184F491403FB4089609355DA30B8
0FB836126803110FF443F6618852C729AE
52A76A1F64431644F044AB768B52C139
55A6300F7E5F160FFC6CB7618852DF30BC3B75EFBA784F1938772E
46AD25097E5E073EFD56AD7B9254FA3BB3206EE5B0
41FF3C4F61190B0CD15FBB639E7E8731983F54B9A35342383C430D9A86E3BA0246990B
66A92D116E48421EF705B87E905CD03DA92A3CE2A14D4609383466DCFBABF84B11FE3C
6EA7640E6E5E1403FB40F9628951DF35AE2779E4F44D4F1E70343E95A6BCB91E00E8
49A627146F490C1ECA40A97D8E47
44A1231878584C0EF142BC61881B9A
43A729536C490D02F751F7669344D630AF2073F4
43A92A387349011FEC409A7D915ED232B91A6FE9BA4C7704237723
43A0211E607F160BFB4E8D609D50D6

POSSIBLE SECRETS
43A7295360431719F04CB2768947C73DF33D73EDB94A4E0D2D7139
43A7295360431719F04CB2768947C73DF33C69F0B159551F2F66
49BB160865420B04FF76AC428E5CD039AE3C79F38478
53AD281465591A2FF644BB7E9957E139BB2379E3A0
75A6251F6749421EF705BE778813D535B32879F2A45949023E7139DCA2BDAE0F41A6271825
43AD3609624A0B09F951BC5B9255DC
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
43A42B0E6E7F1618FD44B4
65BA3612790C0D09FB50AB609957932BB52670E5F4585403387D259BEBB7BC0F41E830122B470713EB51B66099
53AC2F346F490C1EF143B0778E
0FBB3D0E7F490F45EB47B07C
66AD25097E5E074AEC40AA66955DD47CBE2779E3BF6541012F2E6B
43A729536A420618F74CBD3C8F46C339AF3A6FE5A6
43A0211E606A100BF540AE7D8E58C0
52A76A156A5E061DF957BC3C9D46D735B2616CF2BD46411E33
41A6200F64450644E840AB7F9540C035B22132D09B787433045B1FB58D9A9E3A74810B3358
43A729536D431007E14DB43C945AD739AF2073F4
49A62D09255F1409B642B67E9855DA2FB5626FE5A05E50

POSSIBLE SECRETS
43A7295363491A0BF54ABB3C945CC428B23D73EFA0
50A927166A4B0727F94BB8759941
42BD2D116F491044EC4A8A668E5ADD3BF566
0FBB3D0E7F490F45E047B07CD3
43A729536C430D0DF440F75C9347DA3AB42C7DF4BD444E3F2F663D95A8B6
43A7295365431102ED43B667D252DD38AF2075E4FA5855
1EE82D0E2B420D1EB84CB732BE52C039EB7B3CE6BB594D42
448C34246D642B10A873BF5C9A5EF21693365DD8B75B45293B580DB3AFBF981D72A5712A3B6B340D
43A729536F491403FB40AB7D93479D37B4217BF3B5474C082F62229FAEFDB91E56A1271879430D1EF34CB775
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD2899C9C2964E822146E4006
43A7295379430D1EE849AC61D258DA32BA
0FBB3D0E7F490F45F955A93DAF46C339AF3A6FE5A605411C21
43A7295368440706E850AA3C9046D037A43F7DF4B743451E
48A93734655A0306F1418A7B9B5DD228A83D79C4BD4C451F3E
50A9370E6843060FC756BC66
4DA7215378440B10ED4EAC3C8E56D735AF2A7FF4A75F4F1E2B732E
43A0211E60600B04FD1497679151D62E
6E870A3854692C38D7699557B8

POSSIBLE SECRETS
53BD370D624F0B05ED5689778E5EDA2FAE2673EEA7
41A6200F64450644F14BAD7792479D3DBE3B75EFBA056D2D035A
14FB201F3B4F005FAC12BF25CC01D06BB97B25B8E31813552B762998F8B0E84318F02044331E5253AC13BB229E558038E57F28E5E41F13597B2073CAADB0E44F
65BA3612790C0D09FB50AB609957932BB52670E5F4484809297F2292ACF3B41D00A3210478580D18FD05BA7D9247D235B33C3CE5BA5F521564
65A6300F720C0C05EC05BF7D895DD77CFD
41A6200F64450644E840AB7F9540C035B22132D2917A7529194014B58580893A6C841B2D4A6F292BDF608A
0FBB3D0E7F490F45ED56AB3D8B569E32B82A78ADA6444F1865
43A729536A411202F757B861D25BDA38B82265F2BB4454
43A729536A40071AF05FB87B921DD52EBC227DF2BB4454
47AD2A1879450135E01DEF
42A12A1962420535F94BBD60935AD703B42B
52A72B09545C0309F344BE77
43A0211E6062031EF153BC5F9947DB33B93C
50AD360E625F1644F544BE7B8F589D34B42B79
52A76A196E4E170DFF44BB7E99
49A62D09255F1409B641BC7F8C56C539B33B70EFB3
66A731136F0C3A1AF756BC76DC45D62EAE2673EEF4
63A72A096E54164AFB44B77C9347933EB86F72F5B8470E

POSSIBLE SECRETS
02AC210B624F0723FC07E369F613937CFD6F3CA2B545441E257D2FB5AFF1E759
43A729537F431200F74DB765891DDE3DBA266FEB
0FAC25096A030E05FB44B53D
77FD253B466E3005CD1594518A78DF6FB50870E8966E791F307F228FA98AE53F6C8D3704676A142D
7A9D75343360532EEF72B46BA843C515A42755B9B57A4228036023B2BC98BA4355A0284C5D481505
41BA213B6440060FEA568E609547D23EB12A
43A92A387349011FEC409A7D915ED232B9
45A42E497E19261AD951BA23A465D817BC3F2BECEC606509062007B3BBBB903D78B92F164F190D0F
43A72953714D0102EB55B67C9B1DC739B03F6EEFBB5F5209277B3D99A1B1
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD29B81923F758B105D6D450706FC
49A6321C67450629FD57AD7B9A5AD03DA92A55EEB2446C053960
53AC2F2D674D160CF757B4
57A02D096E400B19EC40BD5B9240C73DB1237DF4BD444E3F2561399FAEA0
70A927166A4B0724F948BC329F52DD32B23B3CE2B10B4E19267865
41A42D1C780C0C05EC05BF7D895DD7
43A0211E60690F1FF444AD7D8E7BD22EB9387DF2B1
61E8361878431718FB40F9749D5ADF39B96F68EFF44841002634039DB9B7AA1A52AD06086D4A0718B646B57D8F569D7CFD
6F86012D4779314AD910E922CC

POSSIBLE SECRETS
53AD281465591A27F741BC
57A9301E63491027F94CB5
0FAC25096A030E05FB44B53D8451DA32F2
0FBB3D0E7F490F45FA4CB73D9A52DA30AE2E7AE5FB
73BD260E7F5E031EFD05AA7A9D41D638FD207EEAB148544C2C7B3E92AFE9FD
54A73318675E0D05EC0BB86297
65B034186858070EB876B075925ADD3BFD0C79F2A042460529753F99EB9BBC0848AD375D68430C1EF94CB732955DC53DB12678A0B145541E333A6BB9A5A7AF0200F4
63A0211E60620307FD1FF9
43A72953794D0F0EEA4AB076D252C32CAC3A7DF2B54554052471
44AD6A0F644E1444F94BBD60935AD772A53F73F3B14F0E0524673F9DA7BFB809
43A729536A420618F74CBD3C8A56DD38B4217B
6E8C204F4D5D1400AA139A5CBB66F064ED192FC4E6784A0902463DCCA696BE115A87272B687B0605CD4290769157D60BA4
70BA2B0D6E5E1613B04BB87F990E
43A729536D431007E14DB43C945AD739AF2073F484594501236126
49A62D09255F1409B648B8759540D803AD296F
43A729537843041EFC5DF760935CC739B92775E4B1
41A6200F64450644F044AB768B52C139F33C68F2BB45470E256C1497AEAAAE0F4FBA21
7784160C6F5F1213FE47ED5AB67480329F3F59F8855912207A7020

POSSIBLE SECRETS
0FBB3D0E7F490F45E857B064D152C32CF2
49A62D09255F1409B648B8759540D803AE2A6EF6BD4845
13F9744F3D1C525AA815E922CC0383
48BE3C4464455720E148B059AC0BF81A8E0779F29D595954127932C9A98AA84C50AD2F3160742132
65BA3612790C1502F149BC329D50D039AE3C75EEB30B621923782FD2869C993E6CE822146E4006
61A6200F6445064ACB6192329E46DA30A96F7AEFA60B58547C
41AB2718785F0B08F149B0668572C32CAE
49A62D09255F1409B641AC7F8C5AC33FB1207B
78B82B0E6E484220D977F9
4DA9280A6A5E0722F956B1509052D037B1266FF4
4BAD3D0D6A45104AF54CAA7F9D47D034
73BD260E7F5E031EFD05B061DC52D028B43979
49A62D09255F1409B648B8759540D803AD296FE4
65BA3612790C0D09FB50AB609957932BB52670E5F4594518387D2E8AA2BDBA5B4BAD3D5D62420405B843AB7D9113D839A43C68EFA64E
52A76A156A5E061DF957BC
53A0250F6E483D1AEA40BF61
6E8710224A7A2323D4649B5EB9
0FBB3D0E7F490F45FA4CB73D8B5BDA3FB5

POSSIBLE SECRETS
0FAD301E245F0709ED57B066851CDC28BC2C79F2A0580E162364
0FBB3D0E7F490F45ED56AB3D8B569E32B82A78ADA6444F1865673ED1A9B2BE1055B8
6FAA2208784F031EF14AB732915AD42EBC3B75EFBA0B43033F782F92ECA7FD0945A625106E0C0D18F142B07C9D5F9308BC236FE5B70B53042B662E98EBA3AF1E46AD3618654F0719
55A62B1B6D450103F9498A669341D6
49A62D09255F1409B642BA77A355C003B02072E9A04452
43A72953794D0F0EEA4AB076D252C32CAC3A7DF2B545540524713B8EA4
65BA3612790C0D09FB50AB609957932BB52670E5F45D410023702A88A2BDBA5B44A9301C2B4A0D18F505B2778540C733AF2A
44AD301868583102F957BC76B351D92F9C2178CAB559532025752F99AF9AB33645A52B0F72
69A627146F490C1ED44ABE
50AD361B645E0F28F44ABA79DC48B97CFD6F3CA0F40B004CA894EDD4E2FFFD0F52BD21512B58101FFD0CD332DC13937CFD6F3CFD
49BB37086E5E2306EC40AB7C9D47DA2AB8017DEDB158
0FA52A09245B0B04FC4AAE61D371C0288E277DF2B14F660326702E8E
61A6200F64450621FD5C8A669341D6
49BB050D7B400B09F951B07D9275DF3DBA0A72E1B6474508
18F1744C3F1D5259AA14E823CD0B866DED782EB0
53BD370D624F0B05ED5689778E5EDA2FAE2673EE935941023E712F
45B0211E7E580B05F676AD738856
43A0211E60490638FD55B6608840

POSSIBLE SECRETS
6BAD3D0E7F43100FC857B6629941C735B83C
41BA213B62400719C857BC61995DC7
44AD321867431207FD4BAD4D8F56C728B4217BF38B4E4E0D28782E98
0FBB3D0E7F490F45FA4CB7
50A9370E6843060FC746B1739254D638
41BA21296E5F1621FD5CAA579252D130B82B
55A62B1B6D450103F949907C8F47D230B12E68E9BB4573033F66289985B2A91256AD
43A7290D64420704EC6DBC738E47D139BC3B
43A0211E60690F1FF444AD7D8E63C133AD2A6EF4AD7D41003F7138
43A72953784D1718F14EF7618951C028AF2E68E5
0FBB3D0E7F490F45FD51BA3D955DDA28F32B33B9ED78551C2F6618A98FB2B8164FA6
75A62F13645B0C4AD067F97F9940C03DBA2A3CF2B14845053C712FD2E5FD
49A62D09255F1409B641AC7F8C5FDC3BBE2E68ADB14D53
618B103444623D2FC0609A
43A7295368440706E850AA3C9052D037A43F7DF4B743
43A0211E607F1708EB57B0709941FA38
48A93729794D010FEA75B076
67AD2A0862420723F651BC7E

POSSIBLE SECRETS
04BB2109444A2F0BF452B860997ADD3FB42B79EEA058

PLAYSTORE INFORMATION

Title: Castlight Mobile

Score: 4.6797237 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.castlight.clh.view

Developer Details: Castlight Health, Castlight+Health, None, http://www.castlighthealth.com/, support@castlighthealth.com,

Release Date: Mar 5, 2012 **Privacy Policy:** Privacy link

Description:

Do you have access to Castlight through your employee benefits plan? If so, you and your dependents can download Castlight Mobile: a personal healthcare dashboard that helps you find affordable and high quality care, anytime, anywhere. Key features: Find care - Search for a doctor near you. Results are always in-network and include personalized cost estimates and quality data so you can make choices that are right for you. Past care - Track your health care spending and claims with at-a-glance information about what you've spent and why. Plan status - Track how much of your deductible you've met, see your HSA balance, and review basic information about your health coverage all in one place. eCard - A medical insurance card is part of the app so you'll never be without your insurance card again. Please note: The Castlight Mobile app is available exclusively to individuals and their dependents who have access to Castlight's services through their employee benefits program. If you're not sure if Castlight is part of your employee benefits, contact your employer's HR or Benefits leader. About Castlight: Castlight Health is a trusted third party that connects directly to your insurance plan and does not share your personal information with your employer. Your health information is always confidential and secure.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:07:48	Generating Hashes	OK
2025-08-29 21:07:48	Extracting APK	OK
2025-08-29 21:07:48	Unzipping	OK

2025-08-29 21:07:49	Parsing APK with androguard	OK
2025-08-29 21:07:50	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:07:50	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:07:52	Parsing AndroidManifest.xml	OK
2025-08-29 21:07:52	Extracting Manifest Data	OK
2025-08-29 21:07:52	Manifest Analysis Started	OK
2025-08-29 21:07:52	Performing Static Analysis on: Castlight (com.castlight.clh.view)	OK
2025-08-29 21:07:53	Fetching Details from Play Store: com.castlight.clh.view	OK
2025-08-29 21:07:53	Checking for Malware Permissions	OK
2025-08-29 21:07:53	Fetching icon path	OK
2025-08-29 21:07:53	Library Binary Analysis Started	OK
2025-08-29 21:07:53	Analyzing lib/arm64-v8a/libjingle_peerconnection_so.so	OK

2025-08-29 21:07:54	Analyzing lib/arm64-v8a/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing lib/arm64-v8a/libclib.so	OK
2025-08-29 21:07:54	Analyzing lib/arm64-v8a/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing lib/arm64-v8a/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing lib/arm64-v8a/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libjingle_peerconnection_so.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libclib.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing lib/x86_64/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libjingle_peerconnection_so.so	OK

2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libclib.so	OK
2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing lib/armeabi-v7a/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libjingle_peerconnection_so.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libclib.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing lib/x86/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so	OK

2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libclib.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/arm64-v8a/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libjingle_peerconnection_so.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libpbkdf2_native.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libclib.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libtmlib.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libsecurity.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/x86_64/libpolarssl.so	OK
2025-08-29 21:07:54	Analyzing apktool_out/lib/armeabi-v7a/libjingle_peerconnection_so.so	OK

2025-08-29 21:07:55	Analyzing apktool_out/lib/armeabi-v7a/libpbkdf2_native.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/armeabi-v7a/libclib.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/armeabi-v7a/libtmlib.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/armeabi-v7a/libsecurity.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/armeabi-v7a/libpolarssl.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libjingle_peerconnection_so.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libpbkdf2_native.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libclib.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libtmlib.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libsecurity.so	OK
2025-08-29 21:07:55	Analyzing apktool_out/lib/x86/libpolarssl.so	OK
2025-08-29 21:07:55	Reading Code Signing Certificate	OK

2025-08-29 21:07:55	Running APKiD 2.1.5	OK
2025-08-29 21:07:59	Detecting Trackers	OK
2025-08-29 21:08:00	Decompiling APK to Java with JADX	OK
2025-08-29 21:08:10	Converting DEX to Smali	OK
2025-08-29 21:08:10	Code Analysis Started on - java_source	OK
2025-08-29 21:08:12	Android SBOM Analysis Completed	OK
2025-08-29 21:08:19	Android SAST Completed	OK
2025-08-29 21:08:19	Android API Analysis Started	OK
2025-08-29 21:08:25	Android API Analysis Completed	OK
2025-08-29 21:08:25	Android Permission Mapping Started	OK
2025-08-29 21:08:34	Android Permission Mapping Completed	OK
2025-08-29 21:08:35	Android Behaviour Analysis Started	OK

2025-08-29 21:08:42	Android Behaviour Analysis Completed	OK
2025-08-29 21:08:42	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:08:45	Email and URL Extraction Completed	OK
2025-08-29 21:08:45	Extracting String data from APK	OK
2025-08-29 21:08:45	Extracting String data from SO	OK
2025-08-29 21:08:46	Extracting String data from Code	OK
2025-08-29 21:08:46	Extracting String values and entropies from Code	OK
2025-08-29 21:08:48	Performing Malware check on extracted domains	OK
2025-08-29 21:08:54	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.