ANDROID STATIC ANALYSIS REPORT

No icon

SoundCloud (2024.01.23-release)

File Name:	soundcloud.apk
Package Name:	com.soundcloud.android
Scan Date:	Feb. 5, 2024, 6:46 a.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C
Trackers Detection:	11/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
15	29	3	3	2

FILE INFORMATION

File Name: soundcloud.apk
Size: 77.6MB
MD5: 2a24ce66045233982ba97e6085195036
SHA1: dfa15e0796953fdefc70cb50f934799d021a4f6b
SHA256: 374a8b76b8bc9d9c7cb332cebf3e2a0e5e4914d92a1262446c86820ab0a623ff

APP INFORMATION

App Name: SoundCloud
Package Name: com.soundcloud.android
Main Activity: com.soundcloud.android.launcher.LauncherActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2024.01.23-release
Android Version Code: 225060

APP COMPONENTS

Activities: 58
Services: 24
Receivers: 32
Providers: 10
Exported Activities: 7
Exported Services: 3
Exported Receivers: 7
Exported Providers: 1

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: CN=Jon Schmidt
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-11-30 06:00:46+00:00
Valid To: 2035-11-24 06:00:46+00:00
Issuer: CN=Jon Schmidt
Serial Number: 0x4cf4930e
Hash Algorithm: sha1
md5: 9b4c7012b9adf3d9a33454560751843a
sha1: 13c9e5900d437089b72324b0260f3b5a0b4e027b
sha256: aff930d671fa0a57b8c41d1678cc2a8ea717075a74e346942a140afa441339d2
sha512: 10ba277eb58a5cec33cd39ced0ce121b8ca9f355ccce03f428005b4d870782046c3e1f728e3286ae910e3b6585d19642521976691bcbdacbfddbea3ca6f59cfd
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 35d1f3b25139036753ae70d409475ae8a9cfa0a5b88d954ab0bd55efe3095d4f
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.soundcloud.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check
	Compiler	r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.PRODUCT check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes7.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.soundcloud.android.deeplinks.ResolveActivity	Schemes: http://, https://, soundcloud://, Hosts: @string/host_name, @string/mobi_host_name, @string/firebase_host_name, @string/on_soundcloud_host_name, *, links.announcements.soundcloud.com, links.billing.soundcloud.com, links.confirmation.soundcloud.com, links.notifications.soundcloud.com, links.notifications.soundcloudmail.com, links.soundcloudmail.com, links.account.soundcloud.com, links.hello.soundcloud.com, links.login.soundcloud.com, links.transactions.soundcloud.com, links.messages.soundcloud.com, links.warnings.soundcloud.com, Path Patterns: /uni.*,
com.soundcloud.android.main.MainActivity	Schemes: soundcloud://, Hosts: callback, Mime Types: vnd.soundcloud/search_item,
com.soundcloud.android.onboarding.auth.AuthenticationActivity	Schemes: sc://, Hosts: auth,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.soundcloud.android,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.soundcloud.android://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	soundcloud.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **9** | WARNING: **19** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Service (com.soundcloud.android.playback.players.MediaService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=http://@string/host_name]	high	App Link asset verification URL (http://@string/host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
6	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=https://@string/host_name]	high	App Link asset verification URL (https://@string/host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
7	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=http://@string/mobi_host_name]	high	App Link asset verification URL (http://@string/mobi_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
8	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=https://@string/mobi_host_name]	high	App Link asset verification URL (https://@string/mobi_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
9	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=http://@string/firebase_host_name]	high	App Link asset verification URL (http://@string/firebase_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
10	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=https://@string/firebase_host_name]	high	App Link asset verification URL (https://@string/firebase_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
11	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=http://@string/on_soundcloud_host_name]	high	App Link asset verification URL (http://@string/on_soundcloud_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
12	App Link assetlinks.json file not found [android:name=com.soundcloud.android.deeplinks.ResolveActivity] [android:host=https://@string/on_soundcloud_host_name]	high	App Link asset verification URL (https://@string/on_soundcloud_host_name/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
13	Activity (com.soundcloud.android.deeplinks.ResolveActivity) 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.
14	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Broadcast Receiver (com.soundcloud.android.offline.MediaMountedReceiver) 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.
16	Activity (com.soundcloud.android.main.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Activity (com.soundcloud.android.onboarding.auth.AuthenticationActivity) 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.
18	Broadcast Receiver (androidx.mediarouter.media.MediaTransferReceiver) 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.
19	Activity (com.soundcloud.android.creators.upload.UploadEditorActivity) 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.
20	Broadcast Receiver (com.soundcloud.android.playback.widget.service.PlayerAppWidgetProvider) 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.
21	Content Provider (com.soundcloud.android.playback.image.notification.MediaNotificationContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Activity (com.adswizz.interactivead.internal.action.PermissionActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Activity (com.facebook.CustomTabActivity) 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.
24	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.
25	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.
26	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
27	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
28	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
29	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: 3 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	lk/im.java wj/uf.java xh/a.java
				ag0/k.java aq/t0.java b/a.java bc0/a.java bc0/c.java bc0/l.java bc0/o.java bm0/l.java bo/app/u4.java c70/b.java cn0/c.java cn0/m.java coil/memory/MemoryCache.java com/ad/core/adFetcher/AdRequestConnection.java com/adswizz/common/AdPlayer.java com/adswizz/core/analytics/internal/model/AWSPinpointTask.java com/adswizz/core/zc/model/ZCAnalyticsConnector.java com/adswizz/datacollector/internal/model/SensorModel.java com/braze/Constants.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/braze/models/inappmessage/InAppMessageHtml.java com/braze/models/outgoing/AttributionData.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragment.java com/braze/ui/inappmessage/listeners/DefaultInAppMessageWebViewClientListener.java com/onetrust/otpublishers/headless/Public/Keys/OTUXParamsKeys.java com/snap/corekit/security/SecretKeyFactory.java com/soundcloud/android/data/core/FullUserEntity.java com/soundcloud/android/foundation/ads/AdVerificationResource.java com/soundcloud/android/messages/storage/push/MessageEntity.java com/soundcloud/android/ui/components/buttons/FollowActionButton.java com/soundcloud/android/ui/components/buttons/StandardFollowToggleButton.java com/soundcloud/android/ui/components/buttons/StandardMessageToggleButton.java com/soundcloud/android/ui/components/cards/PersonalizedPlaylist.java com/soundcloud/android/ui/components/cards/UserActionBar.java com/soundcloud/android/ui/components/listviews/comment/CellComment.java com/soundcloud/android/ui/components/listviews/message/CellConversation.java com/soundcloud/android/ui/components/listviews/playlist/CellMicroPlaylist.java com/soundcloud/android/ui/components/listviews/playlist/CellSlidePlaylist.java com/soundcloud/android/ui/components/listviews/playlist/CellSmallPlaylist.java com/soundcloud/android/ui/components/listviews/track/CellMicroTrack.java com/soundcloud/android/ui/components/listviews/track/CellSlideTrack.java com/soundcloud/android/ui/components/listviews/track/CellSmallTrack.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/soundcloud/android/ui/components/listviews/user/CellMediumUser.java com/soundcloud/android/ui/components/listviews/user/CellMicroUser.java com/soundcloud/android/ui/components/listviews/user/CellSlideMicroUser.java com/soundcloud/android/ui/components/listviews/user/CellSlideUser.java com/soundcloud/android/ui/components/listviews/user/CellSlideUserWithAction.java com/soundcloud/android/ui/components/listviews/user/CellSmallMessageUser.java com/soundcloud/android/ui/components/listviews/user/CellSmallUser.java com/soundcloud/android/ui/components/notification/NotificationLabel.java com/statsig/androidsdk/Marker.java com/statsig/androidsdk/StatsigClientKt.java com/statsig/androidsdk/StatsigNetworkKt.java com/statsig/androidsdk/StatsigOptionsKt.java com/statsig/androidsdk/StoreKt.java dt/i.java dt/l.java e/d.java e40/a.java en0/d.java en0/j.java en0/n.java en0/p.java f2/f2.java f2/i1.java gc0/b2.java gv0/m2.java h20/n.java hg0/q0.java hg0/w1.java id/h.java il0/c.java jd0/f.java ke/g.java lb0/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ld/d.java ld/p.java ld/x.java lm0/a.java lm0/c.java ln0/i.java ls0/g.java m/c.java m80/v.java ma0/e.java mg0/a.java mn0/d.java mo0/h.java n80/d.java nb0/f.java o80/h0.java oh0/k.java or0/b.java pp0/c.java r/m.java r9/m.java ru/d.java sp/g.java te0/j.java ue0/m.java ue0/n.java ux/s.java ux/u.java v30/a.java wb0/a.java wd0/i.java wh0/j.java wk0/a.java wk0/s.java wp/a.java x3/h.java x3/t0.java x80/j.java xk0/d0.java xq0/f.java yo/b.java yp/b.java yp/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ze0/b.java zj0/w.java zo/e.java zo/w.java zp/f.java zr0/b.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	aj/e.java ar/d.java bo/app/e1.java bq/c0.java co/datadome/sdk/b.java com/adswizz/core/podcast/AdswizzAdPodcastManager.java com/adswizz/core/streaming/AdswizzAdStreamManager.java com/appsflyer/internal/AFc1jSDK.java com/braze/support/IntentUtils.java com/soundcloud/android/onboarding/auth/ui/authentication/AuthLandingFragment.java com/soundcloud/android/sync/BackgroundSyncResultReceiver.java fn/s.java fx/i.java gv0/c0.java gv0/e0.java gv0/z1.java he/q.java hv0/i.java ik/r4.java jx/k.java jx/m.java kj/a.java kk/g2.java lk/tl.java mw0/a.java mw0/b.java nk/f7.java ns0/g.java nv0/e.java nv0/g.java nw0/a.java pg/q1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rh/y0.java si/s.java uh/b.java uk/kc.java wf/a1.java wf/b1.java wf/c1.java wf/d1.java wf/e.java wf/e1.java wf/z0.java wj/bi4.java wj/ha4.java wj/jf.java xe/w0.java yb/a.java
				ae0/a.java aj/q.java bb/j.java be/i.java ce/i.java com/ad/core/adBaseManager/internal/AdDataImpl.java com/ad/core/adFetcher/AdRequestConnection.java com/ad/core/companion/AdCompanionView.java com/ad/core/streaming/AdManagerStreamingSettings.java com/ad/core/utils/phone/Session.java com/ad/core/video/AdVideoView.java com/adswizz/common/CommonContext.java com/adswizz/common/log/DefaultLogger.java com/adswizz/core/AdswizzCoreManagerSecondProcess.java com/adswizz/core/podcast/AdswizzAdPodcastManager.java com/adswizz/core/podcast/a.java com/adswizz/core/podcast/b.java com/adswizz/core/podcast/c.java com/adswizz/core/streaming/AdswizzAdStre

NO	ISSUE	SEVERITY	STANDARDS	FILES
				amManager.java com/adswizz/core/zc/ZCManager.java com/adswizz/interactivead/InteractivityManager.java com/adswizz/obfuscated/j0/e.java com/adswizz/omsdk/plugin/OmsdkPlugin.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1kSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFe1bSDK.java com/appsflyer/internal/AFe1dSDK.java com/appsflyer/internal/AFe1eSDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1oSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1rSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFf1uSDK.java com/appsflyer/internal/AFf1vSDK.java com/appsflyer/internal/AFg1ySDK.java com/appsflyer/internal/AFg1zSDK.java com/appsflyer/internal/AFh1gSDK.java com/bumptech/glide/Glide.java com/onetrust/otpublishers/headless/Internal/Log/OTLogger.java com/yalantis/ucrop/util/ImageHeaderParser.java d1/a.java dl/d2.java dl/s0.java dl/t.java dl/v.java ec/a.java ec/c.java gc/b.java ge/a.java gg/a.java h11/a.java hb/b.java hd/d.java hd/e.java i01/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ib/a.java ik/l4.java ik/u3.java ik/y.java iu0/a.java jd/b.java jd/h.java jd/i.java k3/m0.java k6/a.java kd/c.java kd/e.java kj/b.java kk/g1.java l4/d.java lc/a.java ld/h.java ld/i.java ld/k.java ld/z.java md/i.java md/j.java mj/a.java mj/b.java mj/h.java mj/q.java mj/u.java mj/x.java mk/v.java mq/d.java mq/d0.java mq/k.java mq/k0.java mq/p0.java mq/s0.java mq/w0.java mq/x0.java n4/o.java nd/e.java nd/i.java o5/o0.java od/a.java pa/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pd/c.java pd/d.java pd/g.java pd/t.java pd/u.java pd/v.java q4/f.java qe/l.java qm/s.java rd/h.java s5/l.java sd/c.java sd/d0.java sd/f.java sd/g0.java sd/n.java sd/p.java sd/q.java sd/u.java sv0/b.java uk/t4.java uo/g.java w0/m.java wd/a.java wd/c.java wd/h.java wj/ff0.java wj/o23.java wj/oa.java wk/a.java wm/i.java xa/d.java xa/e.java y4/o.java yd/e.java yd/n.java yd/o.java yk/a.java zd/d.java zk/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/comscore/android/CommonUtils.java com/comscore/android/util/jni/AndroidJniHelper.java kk/f6.java qm/c.java wj/d33.java wm/w.java xo/i.java zj/l1.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	hq/c.java k6/a.java p7/d0.java vc0/u.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ik/k0.java ik/l0.java ik/o5.java ik/p5.java kg/m0.java kg/t0.java rg/d.java rg/e.java si/f.java si/l.java uk/n.java uk/q4.java uk/s.java uk/vc.java uk/wb.java w7/c.java wj/ex1.java wj/sy1.java wj/zx1.java xp/o3.java xp/p2.java xu/b.java xu/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/b0.java bo/app/d6.java bo/app/e.java bo/app/f1.java bo/app/g6.java bo/app/h4.java bo/app/l0.java bo/app/l1.java bo/app/m.java bo/app/m0.java bo/app/m6.java bo/app/n0.java bo/app/r3.java bo/app/v5.java bo/app/w4.java bo/app/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java com/statsig/androidsdk/StatsigClient.java he/a.java he/i.java he/m0.java he/o0.java he/y0.java hf/x.java oe/j.java ue/b.java wu/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	at/b.java com/mattprecious/telescope/TelescopeLayout.java com/yalantis/ucrop/util/FileUtils.java j5/i.java nk/w2.java wj/dm.java wj/dq.java wj/dr.java xe/w0.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	aq/m.java com/adswizz/core/podcast/AdswizzAdPodcastManager.java com/braze/support/StringUtils.java com/comscore/android/id/IdHelperAndroid.java com/comscore/util/crashreport/CrashReportDecorator.java ie/d.java ik/r3.java lk/lk.java qe/l.java ss0/a.java uk/kc.java wj/be.java wj/gk.java wj/ye0.java
11	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/comscore/util/crashreport/CrashReportDecorator.java gf/a.java hq/b.java lk/n.java m50/m.java mq/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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/soundcloud/android/listeners/dev/DevDrawerFragment.java de0/c.java dv/c.java l3/e.java po0/b.java u/j0.java
13	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	h01/c.java h01/d.java h01/i.java h01/j.java
14	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1tSDK.java com/segment/analytics/a.java
15	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	co/datadome/sdk/CaptchaActivity.java com/soundcloud/android/insights/a.java com/soundcloud/android/onboarding/auth/c.java wj/ml0.java xa/e.java
16	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	ai/h.java
17	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	kk/s6.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__vsnprintf_chk', '__FD_SET_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__FD_CLR_chk', '__FD_ISSET_chk']	False warning Symbols are available.

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

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__memmove_chk', '__strlen_chk', '__read_chk', '__vsprintf_chk', '__strcat_chk', '__strchr_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi-v7a/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	armeabi-v7a/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	armeabi-v7a/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	armeabi-v7a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	armeabi-v7a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	armeabi-v7a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	armeabi-v7a/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	armeabi-v7a/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strcat_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__strchr_chk', '__strlen_chk', '__memcpy_chk', '__vsprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86_64/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86_64/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86_64/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	x86_64/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86_64/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86_64/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__vsnprintf_chk', '__FD_SET_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__read_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	x86/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	x86/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	x86/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	x86/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	x86/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	x86/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	x86/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	x86/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	x86/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__vsnprintf_chk', '__FD_SET_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__FD_CLR_chk', '__FD_ISSET_chk']	False warning Symbols are available.

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	arm64-v8a/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	arm64-v8a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	arm64-v8a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	arm64-v8a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	arm64-v8a/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__memmove_chk', '__strlen_chk', '__read_chk', '__vsprintf_chk', '__strcat_chk', '__strchr_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	armeabi-v7a/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	armeabi-v7a/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	armeabi-v7a/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
58	armeabi-v7a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	armeabi-v7a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
60	armeabi-v7a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	armeabi-v7a/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	armeabi-v7a/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strcat_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__strchr_chk', '__strlen_chk', '__memcpy_chk', '__vsprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	x86_64/libsignup-signature-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	x86_64/libkiss-fft-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
66	x86_64/libcrasher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	x86_64/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
68	x86_64/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
69	x86_64/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
70	x86_64/libcomScore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
71	x86_64/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
72	x86_64/libflipper_shared_android_6.0.13.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__vsnprintf_chk', '__FD_SET_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__read_chk', '__memmove_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.GET_ACCOUNTS, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	4/45	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
soundcloud-com-soundcloud.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
developers.google.com	ok	**IP:** 142.250.189.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.content.text	ok	No Geolocation information available.
android.googlesource.com	ok	**IP:** 142.251.2.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.statsig.com	ok	**IP:** 34.120.214.181 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
telemetry.soundcloud.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.google-analytics.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.soundcloud.com	ok	**IP:** 108.138.246.26 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.recaptcha.net	ok	**IP:** 142.250.189.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
eventgateway-staging.lb.db.s-cloud.net	ok	No Geolocation information available.
soundcloud.com	ok	**IP:** 18.155.192.45 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.protocol.https	ok	No Geolocation information available.
www.care.com	ok	**IP:** 69.192.139.95 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.363598 **Longitude:** -71.085205 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
us-central1-gcp.api.snapchat.com	ok	**IP:** 35.190.43.134 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.soundcloud.com	ok	**IP:** 65.8.161.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
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
segment-data-us-east.zqtk.net	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.251.46.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
promoted-staging.soundcloud.com	ok	**IP:** 13.227.74.27 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.protocol.file	ok	No Geolocation information available.
csi.gstatic.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
events-api.soundcloud.com	ok	**IP:** 34.111.175.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api-auth.soundcloud.com	ok	**IP:** 18.155.202.23 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
pages.soundcloud.com	ok	**IP:** 18.244.214.65 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 157.240.22.19 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
goo.gl	ok	**IP:** 172.217.164.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pandora.com	ok	**IP:** 208.85.40.158 **Country:** United States of America **Region:** California **City:** Oakland **Latitude:** 37.810181 **Longitude:** -122.269073 **View:** Google Map
udm.scorecardresearch.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
va.sndcdn.com	ok	**IP:** 18.239.199.93 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.mtv.com	ok	**IP:** 23.37.17.98 **Country:** Philippines **Region:** Cebu **City:** Cebu City **Latitude:** 10.316720 **Longitude:** 123.890709 **View:** Google Map
sb.scorecardresearch.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
crash-trace.s-cloud.net	ok	**IP:** 13.227.74.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
bugs.java.com□□□□□□□□□□□□□□	ok	No Geolocation information available.
statsigapi.net	ok	**IP:** 34.120.214.181 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api-lakza6i6pq-ew.a.run.app	ok	**IP:** 216.239.36.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.protocol.systemresource	ok	No Geolocation information available.
admob-gmats.uc.r.appspot.com	ok	**IP:** 142.251.214.148 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.protocol.verbatim	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cdn.pixabay.com	ok	**IP:** 104.18.40.96 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
sviap.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.google.com	ok	**IP:** 142.250.188.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
zc.adswizz.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
console.statsig.com	ok	**IP:** 34.36.101.214 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
google.com	ok	**IP:** 142.251.32.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sars.s	ok	No Geolocation information available.
bugreport.java.com□java□□□□□□□□□bug□□□□□□□□□□□□□	ok	No Geolocation information available.
api-mobile.soundcloud.com	ok	**IP:** 18.239.192.35 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
googleads.g.doubleclick.net	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
imasdk.googleapis.com	ok	**IP:** 142.250.189.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
storage.googleapis.com	ok	**IP:** 142.251.32.59 **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.
app-measurement.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 142.251.46.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sondheim.braze.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
api-sdk.datadome.co	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
crashpad.chromium.org	ok	**IP:** 142.251.46.243 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
b.scorecardresearch.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
mobile-data.onetrust.io	ok	**IP:** 104.18.32.193 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
graph.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
www.content.image	ok	No Geolocation information available.
schemas.google.com	ok	No Geolocation information available.
cookies2-ds.dev.otdev.org	ok	No Geolocation information available.
insights-ui.soundcloud.test	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
clickthrough.visualad.com	ok	**IP:** 198.58.118.167 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
sdlsdk.s	ok	No Geolocation information available.
insights-ui.soundcloud.com	ok	**IP:** 18.173.121.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.protocol.ftp	ok	No Geolocation information available.
api-mobile-staging.soundcloud.com	ok	**IP:** 108.138.246.107 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
secure.soundcloud.com	ok	**IP:** 18.238.192.19 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.snapkit.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
graph.soundcloud.com	ok	**IP:** 99.84.238.190 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
test.com	ok	**IP:** 67.225.146.248 **Country:** United States of America **Region:** Michigan **City:** Lansing **Latitude:** 42.733280 **Longitude:** -84.637764 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.yahoo.com	ok	**IP:** 69.147.88.7 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.251.46.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.251.32.42 **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.
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
adservice.google.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
googlemobileadssdk.page.link	ok	**IP:** 142.250.191.33 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
demo.deliveryengine.adswizz.com	ok	**IP:** 13.227.74.85 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.protocol.doc	ok	No Geolocation information available.
www.protocol.gopher	ok	No Geolocation information available.
sdk.iad-01.braze.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
help.soundcloud.com	ok	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.protocol.netdoc	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.britishmodelbuses.com	ok	**IP:** 91.136.8.128 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
url.com	ok	**IP:** 172.67.169.109 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.content.audio	ok	No Geolocation information available.
www.sqlite.org	ok	**IP:** 45.33.6.223 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.251.46.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.soundcloud.com	ok	**IP:** 18.155.202.41 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.250.189.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
waveform.url	ok	No Geolocation information available.
s3-us-west-2.amazonaws.com	ok	**IP:** 52.218.169.40 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
facebook.com	ok	**IP:** 157.240.22.35 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
www.protocol.jar	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
slaunches.s	ok	No Geolocation information available.
www.protocol.http	ok	No Geolocation information available.
www.http	ok	No Geolocation information available.
i.kym-cdn.com	ok	**IP:** 208.111.152.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
www.pandora.com	ok	**IP:** 208.85.41.59 **Country:** United States of America **Region:** California **City:** Oakland **Latitude:** 37.810181 **Longitude:** -122.269073 **View:** Google Map
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
bugs.java.com	ok	**IP:** 104.89.231.222 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
geolocation.1trust.app	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
i1.sndcdn.com	ok	**IP:** 13.227.74.108 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
bugreport.java.com	ok	**IP:** 104.89.231.222 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
advertising.soundcloud.com	ok	**IP:** 108.138.246.72 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
appleid.apple.com	ok	**IP:** 17.111.105.242 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
docs.google.com	ok	**IP:** 142.250.191.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.protocol.mailto	ok	No Geolocation information available.
ssl.google-analytics.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
cdn-settings.segment.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.snapchat.com	ok	**IP:** 34.149.46.130 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
john@doe.com	w20/g.java
android-beta-logs@soundcloud.com android-dev@soundcloud.com -alpha-logs-playback@soundcloud.com d-beta-logs-playback@soundcloud.com	z10/a.java
email@email.com	com/soundcloud/android/comments/compose/ExperimentalCommentsActivity.java

EMAIL	FILE
ftp@example.com	apktool_out/lib/x86/libflipper_shared_android_6.0.13.so
ftp@example.com	apktool_out/lib/arm64-v8a/libflipper_shared_android_6.0.13.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libflipper_shared_android_6.0.13.so
ftp@example.com	apktool_out/lib/x86_64/libflipper_shared_android_6.0.13.so
ftp@example.com	lib/x86/libflipper_shared_android_6.0.13.so
ftp@example.com	lib/arm64-v8a/libflipper_shared_android_6.0.13.so
ftp@example.com	lib/armeabi-v7a/libflipper_shared_android_6.0.13.so
ftp@example.com	lib/x86_64/libflipper_shared_android_6.0.13.so

TRACKERS

TRACKER	CATEGORIES	URL
AdsWizz		https://reports.exodus-privacy.eu.org/trackers/41
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
ComScore	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/56
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
MoEngage	Analytics	https://reports.exodus-privacy.eu.org/trackers/268
Segment	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/62

HARDCODED SECRETS

POSSIBLE SECRETS
"audio_ad_inject_no_image_lb_key" : "audio_no_image_lb"
"graphql_api_base_url" : "https://graph.soundcloud.com/"
"key_email_notifications_tips" : "tips_mail"
"audio_ad_injection_html_leave_behind_key" : "audio_leave_behind_html_type"
"key_email_notifications_likes" : "likes_mail"
"key_clear_cache" : "clearCache"
"key_push_notifications_reposts" : "reposts_mobile"

POSSIBLE SECRETS
"datadome_client_key" : "7FC6D561817844F25B65CDD97F28A1"
"firebase_database_url" : "https://soundcloud-com-soundcloud.firebaseio.com"
"google_api_key" : "AIzaSyAdgWP9wC36Ays-Gr3cB9o-Rxyi6KRbF4Q"
"dev_drawer_all_share_options_key" : "dev_drawer_all_share_options_key"
"audio_ad_pod_inject_submit_key" : "inject_audio_ad_pod"
"profile_bottomsheet_unblock_user" : "Blocked"
"key_email_notifications_groups" : "groups_mail"
"dev_drawer_section_experiments_layer_prefix_key" : "experiments_layer_%s_"
"client_id_web_auth" : "SSdQ80vM8nLPhbDBylHl2JFK6ElhBr9B"
"private_label" : "Privat"
"obfuscated_client_secret" : "NykCWyEEEyUrRCd2AQAtEAUdfy9HKAAkKRwjJh4cMSk="
"adswizz_ad_position_queue_start_key" : "adswizz_ad_position_queue_start"
"key_email_notifications_follows" : "follows_mail"
"profile_bottomsheet_unblock_user" : "Geblokkeerd"
"adswizz_audio_inject_key" : "adswizz_inject_audio"
"dev_drawer_section_experiments_key" : "experiments"

POSSIBLE SECRETS
"dev_drawer_category_actions_key" : "actions"
"dev_drawer_ad_timer_monitor_key" : "dev_drawer_ad_timer_monitor_key"
"dev_drawer_suggested_follows_key" : "suggest_with_genres_screen"
"video_ad_inject_submit_key" : "inject_video"
"adswizz_force_skip_mode_enabled_key" : "force_skip_mode_enabled"
"key_offline_storage_limit" : "offline.storageLimit"
"adswizz_force_skip_offset_key" : "force_skip_offset"
"com_braze_api_key" : "a16b00df-fc7c-487c-a034-290cf918bf2a"
"private_label" : "Privata"
"key_email_notifications_all" : "all_mail"
"video_ad_injection_html_leave_behind_key" : "video_leave_behind_html_type"
"private_label" : "Privado"
"com_braze_firebase_cloud_messaging_sender_id" : "984739005367"
"audio_ad_injection_companion_key" : "audio_companion_type"
"audio_ad_inject_small_image_companion_key" : "audio_image_companion_centred"
"adswizz_audio_companion_key" : "adswizz_audio_companion_type"

POSSIBLE SECRETS
"gma_dev_drawer_open_ad_inspector_key" : "open_ad_inspector"
"key_push_notifications_follows" : "follows_mobile"
"audio_ad_inject_html_companion_non_responsive_key" : "audio_html_companion_non_responsive"
"key_push_notifications_comments" : "comments_mobile"
"profile_bottomsheet_unblock_user" : "Zablokowano"
"adswizz_audio_ad_pods_inject_key" : "adswizz_inject_audio_ad_pod"
"profile_bottomsheet_unblock_user" : "Bloccato"
"audio_ad_inject_large_image_companion_key" : "audio_image_companion_full_bleed"
"consent_show_banner_key" : "consent_banner"
"key_offline_collection" : "offline.offlineCollections"
"gma_dev_drawer_show_native_prestitial_key" : "show_native_prestitial"
"adswizz_ad_position_key" : "adswizz_ad_position_key"
"dev_drawer_immediately_skippable_ads_key" : "dev_drawer_immediately_skippable_ads"
"adswizz_force_timer_duration_key" : "force_timer_duration"
"private_label" : "Privé"
"profile_bottomsheet_unblock_user" : "Gesperrt"

POSSIBLE SECRETS
"adswizz_video_ad_pods_inject_key" : "adswizz_inject_video_ad_pod"
"dev_drawer_upsells_and_conversion_key" : "upsell_and_conversion_category"
"adswizz_video_inject_key" : "adswizz_inject_video"
"dev_drawer_category_design_key" : "design"
"audio_ad_inject_no_html_lb_key" : "audio_no_html_lb"
"key_push_notifications_suggestions" : "recommendations_mobile"
"key_email_notifications_surveys" : "surveys_mail"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"upload_metadata_privacy_switch_private" : "Privado"
"upload_metadata_privacy_switch_private" : "Private"
"key_offline_remove_all_offline_content" : "offline.removeAllOfflineContent"
"key_email_notifications_suggestions" : "recommendations_mail"
"dev_drawer_player_key" : "player"
"profile_bottomsheet_unblock_user" : "Bloqueado"
"private_label" : "Prywatny"
"adswizz_ad_position_mid_queue_key" : "adswizz_ad_position_mid_queue"

POSSIBLE SECRETS
"mobile_api_base_url" : "https://api-mobile.soundcloud.com"
"upload_metadata_privacy_switch_private" : "Privé"
"audio_ad_inject_submit_key" : "inject_audio"
"auth_api_base_url" : "https://api-auth.soundcloud.com/"
"google_crash_reporting_api_key" : "AIzaSyAdgWP9wC36Ays-Gr3cB9o-Rxyi6KRbF4Q"
"audio_ad_injection_image_leave_behind_key" : "audio_leave_behind_image_type"
"key_push_notifications_surveys" : "surveys_mobile"
"audio_ad_injection_companion_html_key" : "audio_companion_has_html"
"com.google.firebase.crashlytics.mapping_file_id" : "97e1717c5f454e2d8ad62da5665aa4cb"
"ad_injection_letterbox_key" : "letterbox"
"dev_drawer_recaptcha_override_key" : "dev_drawer_recaptcha_override_key"
"key_email_notifications_comments" : "comments_mail"
"upload_metadata_privacy_switch_private" : "Privata"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"gma_dev_drawer_show_html_prestitial_key" : "show_html_prestitial"
"video_ad_inject_image_lb_key" : "video_image_lb"

POSSIBLE SECRETS
"video_ad_inject_no_html_lb_key" : "video_no_html_lb"
"video_ad_inject_skip_offset_key" : "video_skip_offset"
"public_api_base_url" : "https://api.soundcloud.com"
"audio_ad_inject_skip_offset_key" : "audio_skip_offset"
"ad_injection_video_type_key" : "video_type"
"profile_bottomsheet_unblock_user" : "Blockad"
"dev_drawer_about_key" : "about"
"dev_drawer_identify_key" : "dev_drawer_identify"
"key_push_notifications_all" : "all_mobile"
"consent_copy_consent_string_to_clipboard_key" : "copy_consent_string"
"audio_ad_inject_no_companion_key" : "audio_no_companion"
"audio_ad_inject_html_companion_responsive_key" : "audio_html_companion_responsive"
"upload_metadata_privacy_switch_private" : "Privat"
"profile_bottomsheet_unblock_user" : "Bloqué"
"ad_injection_fullscreen_key" : "fullscreen"
"dev_drawer_event_logger_monitor_key" : "dev_drawer_event_logger_monitor_key"

POSSIBLE SECRETS
"audio_ad_inject_no_html_companion_key" : "audio_html_no_companion"
"apps_flyer_dev_key" : "6zXGFmoiMQM8PH48fn7nTQ"
"dev_drawer_firebase_debug_key" : "dev_drawer_firebase_debug_key"
"consent_region_code_key" : "consent_region_code"
"ad_injection_video_key" : "video_ads"
"firebase_host_name" : "soundcloud.app.goo.gl"
"private_label" : "Private"
"consent_country_code_key" : "consent_country_code"
"key_sync_wifi_only" : "syncWifiOnly"
"adswizz_audio_no_companion_key" : "adswizz_audio_no_companion"
"gma_dev_drawer_test_device_id_key" : "test_device_id"
"upload_metadata_privacy_switch_private" : "Prywatny"
"adswizz_force_timer_mode_enabled_key" : "force_timer_mode_enabled"
"key_offline_wifi_only" : "offline.wifiOnlySync"
"key_push_notifications_tips" : "tips_mobile"
"adswizz_audio_image_or_html_companion_key" : "adswizz_audio_image_or_html_companion"

POSSIBLE SECRETS
"audio_ad_inject_image_lb_key" : "audio_image_lb"
"consent_restart_to_configure_key" : "consent_restart_to_configure"
"video_ad_inject_html_lb_key" : "video_html_lb"
"video_ad_injection_image_leave_behind_key" : "video_leave_behind_image_type"
"account_authority" : "com.soundcloud.android.provider.ScContentProvider"
"key_push_notifications_likes" : "likes_mobile"
"firestore_api_key" : "AIzaSyC2c83S7cm8L7n0UnI2vqnIKn0as2UN6CE"
"video_ad_inject_no_image_lb_key" : "video_no_image_lb"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"dev_drawer_user_activation_key" : "user_activation"
"dev_event_logger_monitor_mute_key" : "dev_event_logger_monitor_mute_key"
"key_email_notifications_reposts" : "reposts_mail"
"moengage_key" : "8WUYJAML31R2SWQ1SYQU8Y3A"
"ad_injection_audio_ad_pods_key" : "audio_ad_pods"
"dev_drawer_suggested_popular_follows_key" : "suggest_popular_screen"
"upload_metadata_privacy_switch_private" : "Privada"

POSSIBLE SECRETS
"obfuscated_client_secret_web_auth" : "Pg0bIiANHi88RxlgQWAnFAcyAR4kMgYlMGMYL20eMGs="
"dev_drawer_flush_eventlogger_instantly_key" : "dev.flushEventloggerInstantly"
"ad_injection_audio_key" : "audio_ads"
SXEqPPoGCAhkrwWNonsWzEV+zX6m6TBLFFDVOqk+hqA=
8UC+BMIoCN+KAKrN9TZmuJsGMmo3RUHS+FjVMSp9QfgjxjGZ10kqO/oSdOn5Rw29
264a808724eb85f39f27ca8b4cbb8212
5edb9cb29cd9a168c3867b6fd7631c7f
B3EEABB8EE11C2BE770B684D95219ECB
fUXpTL496nlEwFWDjJss3QGGSMP1brRky/zh6LpetKA=
49a567bfcd92712ab01f3d43e62d8778
4bda7bd44dd599319f41ab84e2b1a32d
ZVHCdOeJUA1S4bCrFb9VMsUCP8Sf65wDnbBE+q4M36k=
7Q6sBeEdJYI+qvX8cIFUZRRQ8J+ckQm34FYdYCYSS2Q=
qUEdP6yfmpdCkPVqoE8EyrX/MPjGh4YKRo5g3kOeMoc=
bBmsyCj4vQqoPhkiTKWAfAhlVNxJgrtws7pZHadifrc=
zmLnsak1Fo/LHy30EeWswBCxcOoFKuH08l3DkSTUgzb476o6nI+C8ZUC+d8tLJwZ

POSSIBLE SECRETS
1eWk7vHD3Ee+FybzKEoWLH07Pvdxo5flYR768ntLvpJZNSFjE7xgNzi+al9tiZC4
MFx5XmsCEHtBCjMNFVV6AGUhUBVHWxYIBTU3AGxaXzg=
37a6259cc0c1dae299a7866489dff0bd
Et5K8MZEoJYE/LdMCgxh0i7wX7GVWBBs6Isd533FNz4=
8691a185366081d09d8d7a96fdcb45a2
Eg2eC3eNesWzbAUINzxj1mXRcYgmzS654CxZFoVQbAM=
sha256/O4rGMvpV1NfGyWRRTZ6v92jubDQNBdwlK+E35oZJ9qo=
QfNmx51vMYu7RTw3f+TZAS23f16Jqr3kM4ALSpqOw0Y=
eb2ddbcad1a33c968f7a7947b70eef32
oOIFXcRPpX8LfJq50/GOu7yJ8Zd8cAWeHAa6OVB78FPJKt0W3zZLCFS9LAEUOvnB
d457b1ace33df944d192785120cabdd2
Jz2tk/JKeGJKcc4wwXH5Pf6ZM64fYgV4wWxByPOgNQE=
uNsygnspdKDmMOnOPr9Pza3D3EK7R75fzmNVkfwdpkg=
hMVcCX1S6+m7rVEDNdCHhVgXRFILMOQ9RgLSmTdPHeNgAU8CbmBsymKBuqLQcQaU
ba681c440f4e9b52570a7c79415d4596
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

POSSIBLE SECRETS
9b8f518b086098de3d77736f9458a3d2f6f95a37
14b923690ec5dff68fc0cc06c7fcb69e
fab30f59-2727-4373-b1a8-f0f014a52760
cb7f6f08b0d923c4cebd41a7a3aba420
b5d9f81aa483f701572f47a0ffe81ccc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
7qOZVP58PfP3kLkbSBo98onihlohkIEpZC40FvE5nnCJ8ryn0NERK9JAnlww55zq
9bfbb83ee80ccdee95e73bc93dacd62f
1OxyLDHu2cwu0U7XKtDO3q+DghLeQ8xcTgpGCDWDuEeCcfs+HPxSt8kldIfiq1K0
Q+fOnDUQnIPH75lusFutOgWOI4DeJ6z7X13oo1pZ5m19Kfyi56UOJglWSBqO3AzA
93eE6DMOIbdNN+XzPfwTeV3VtXW82G23sIL9X3G1CFc=
nIX5dAPvXYWFIvHlyxyLt0TnZ91UnAjFxZwf2qcoWSGcs+p5B5p88VCOzepPfMpE
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740 28291115057151
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
fxU2A2MjpZ4aJWGzXeMNURilSCaKosw3oXImrqnhSVmXB+tMi32JakdNlHCV3t0c
bObXLZFRWAdU6+me08AeNX2ciqxi45ddv3QSqAplzos=

POSSIBLE SECRETS
6ecd9c79118932523b4a8ae2442e0f65
sjJJMjdJ4ejENjGN3VSKrjMe8gO2ipNVGbEWPt320LzidWuv9Vye4oanMfYCO4eP
iibTgWRTbrwM2W7HZGJP5cjM0DLiCyA9TVVy1genRaa4nvgE3+CiRN/Fx87DVDsO
0f806da86321144e6c5df8a109f84e0b
NMP1pkZrrrrQ0P+ZBWjqO+z0j/WpBuzawmkUKjAkUeiPRyMNSyS1dkwhVpRyfOJm
y+BEEb1lYOUGwTehZ9VIg/2gibmtEOjDZzKXHhs5BV0=
XCj6cS5OVeEeObzd394PGDbjTuQh+vSye2UT6221ugsKtO2/oznWOSes2cnebrVR
9cb89cc4778b065232cab45b20092995
9mv9Ihk+HlE8P3WJWSjhrxWrdB7cEu1gaxdteA5kBJ6DKumpWYk1Q5Vf8aocVg4i
SMfJnKfhfLLyTw7dzHC+3CXVRNFLWK4N2mQHKB3gm/o=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
71bb3f820c65b6d7142c83047de4d091
NOrE2caDXO4nkFR2Fjy7NgGPKtPlIg1WAorknI/US68=
fbH/fa1wW07iSX89yPc9WELG9OXmO7CRAKCAHB+qo5oZEtCfcaUJh4I9rxcwLdCb
HSZqqXAvfM6p9uyg5JhDHQlMlgQJzMAOkGc0u97KAICZfvxto4YfGWg7De8vgAj2
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

POSSIBLE SECRETS
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
b594f99a4f075810c2a651360e409135
s7rU1m4XsqJ83s2reljdkboWJYkg+gYouDrDcn3Ghpw=
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
sha256/8ca6Zwz8iOTfUpc8rkIPCgid1HQUT+WAbEIAZOFZEik=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3PwoDnm3HnsskB+3ZnJHoZ7BzV0InxUqaAwJBlSwKFs=
RSyr2AK130nKbepDTsaNV0Uv17TWUb4O6ebIiV3GgVs=
w5tjCRfZfXWJzckDvIkXwf5aGJEVejLzfxhnwyqJH5E=
7m0w40FyWBTdaJl9AjXhb9wQqUd7oM1ZB0Gz0iv7tis=
leMw6wdbg7yTx0Ew+oCz/A25ggsdiYC0Nz8e1tg0+qk=
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
ie6hg5HFEpuWzwNgwITo5zXW2wrs4LH8lgFkpMwMO4M=
A7zcecnbEz2swWqo3WVKoAX31f8JEZNN1OTPmTjY02NSqN3cKNpjtt6CyXhCVvfg
3ac60dbe5be17bd607b68a70b51731f3
fbf350f3f12100834cc13c37939d28f6

POSSIBLE SECRETS
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
Ee4p/yPQz67p3LoSNbpt1G8K9rDuoWxBYT8E4CbWyr8=
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
MIrDuKB7N0O22daoYjLtFOJg5TtVRHK1+0ktwmGNtdU=
zahwJ4oRFMB+Gn9BGkfZDZ8TzDEfKTB8Y6I4bT4vlwkVFXvqlnkWd7htbiUzWQyR
VkIjYfvMq2U4v0IdSD1vtjuncSVbXnhZtOloUMiR773TMhx1yeYhN8YLnkrx
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
I5l5b06e/m6OPcJVryww5aceHDWuWNMRDm4mYVrBvJQ=
2+LdC0cYaqAwYHmCPPvRLMkFDbEQiwTEweQcBW/SUlU=
BxKk+MigL5QcJoHkNRs0ALc6QE50Izh8oVpecosSZ5s=
8A6/EDFVHoT40S+hatGoptnyThtgSNe3d9RgnDPM1sB7IlgQEsqPlgL1Jhl6dC4s
Y0trGqGVEUAa7A3LYgSQFKe4N9h1BuTC7OKFYCHfLSg=
ZHFOx+FjaOsul7gEkIcfA8auDnyRWXmT0qbiHVEO6U1RLulNSOFK3tPEgm+pvQxr
bde3b1939d63d0bdf1105e0074dfb167
V4g/Ba6gBXaRd5ZffRmw+I91AzQgJ5Lh37aLVyVGSOY=
os/73Qwr79ouqjFLpLjJlgtKKsT75hksFSajjoaerIA=

POSSIBLE SECRETS
5a44739cd1f2e4aaa494ccceff3e3ecc
TZLhLjkSWa88s5Ub32Va4FnAdRMP/dTQp+jLbB+9PU0=
ScPYVWHkyWrhYKkYpKqrVrn2H6TpKiDLxnPESxYOr/U=
4ac499305db8fa07a0569f776b863868
515523e835962311368053d7bd889d94
sha256/WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
cfa275e115bb4df6529446c2cfe37675
8a1c2ed056d45952c242dbd8dc832869
ae2044fb577e65ee8bb576ca48a2f06e
6IEdtyxtLHwQ4VrfZ9FeCKXP/aP8l8OcsmRcYSdTi2JmfIxazq45FzX1HGkFEJgb
c2686e5853ee5875505bfd79101afccf
M+JigCCNgE9WH1drVXVCETLYEk7iaWPFwZXUH8JlEbE=
ttuIHg/yfWDxJlotLoMLf9WBnVTbWFFKY03C8KHR8FAhIQHccw4LaDLJatYkpo23
gL88T2vBvJS+jBemUvhPpVS5IeaU7cU4wFVgyT6PJl7pFldWXOd3mZxVZlQUSll5
gzR6fJL0MpYPfJ/UkFL9UHjS7jlytQ+eyVRsQJTsxzK4yqDaskM4UtldyBDUp+Z9
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

POSSIBLE SECRETS
E+SzUAEY63zbszVCob40KJ+9dmIewoObuvdjjndY+XY=
1fee7f05ecb471a8659ad73f2fc94dd6
115792089210356248762697446949407573530086143415290314195533631308867097853951
beFEMZ/YBSUug4MSXb2BKymKiM6ZxOOlxExWa37jMlM=
2e46140024a43d3464a5c2a7d7afc5f1
6LeSKgAVAAAAAHZns91dpWFUZzzvM0OUXTLnqmai
KHu8Xbxzr2mu9S25CNgKE5zXBf18Zj2waiAPYoFRjyhOXCyg+mYLv2x/JjCH7GjX
b56e0718dcc3d57a69e9ea9b05940ffe
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
2m6PXcXEiAGusXS1ajjgFu9K1U9p6obL/gDG6se9LFdmc45IuOdD+G2rJwfF1UCD
P45pDuSCFxliLUZXPnwGJMc6aor1Hy6W6MljaMLINPUk74fzm7mVCel744RvNHnU
s1ejGoWFNJedDDJqGqL3B22F5ZMvy0oaymBcWJepS9Hv4/6KtsHBpmbtFfwgqqen
69e96a179afaeb9aba185e0a1d48e88a
A3EfeXObjqx38Tdc4wdTZSQNpfpw6YVck+944M4A/m0=
daqH0kaQsjOZO0MCcjtalDHoDE4Fma0yQGSHO+ub6NM=
fb3OlLRM7e1GWXw1pgCRp7yxLrLt+HeY8mbhCjTXXm8=

POSSIBLE SECRETS
sha256/uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
r6m9xWOlfK6iHuNH3QiJQf71aQCKDM6NhABQId+yaKg=
09e2678ff8377caf12905021e521ef19
iZXNXN9xUbn1GVaYCV3sL1wKWUe/HGVr+Kc3Vh94EyUz5Y8L5QIgpXYgDdLj2Tdj
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
5e91383eac4f0f6b8cdba8fb5c2a4cc0
MaMum1gy44m6JY9Yl3WvxKuatqxbLd+TDTFZCPGq8yp5qgeEGUri2jXkJQRPEPHe
1ZhioNexfONxLbr8oNixHPTbX/qv3RsJiyYoeeb0m+g=
jrfJs+Yxsv/gGQ+cGnmY8EkHVJn84HokHsebN4IZy0eeE0ECK9wrDY7bM1U167G5

POSSIBLE SECRETS
kG8kAzeUJFSjvYuRDtJkr7owBxy52vKH1yfYPq05BRQDWSz1Oa+VomdlwOHttvWk
W3XZxcuCkVWMGpB7rckmrrZNc8kIRKZXHq2IDWH2bOmQhacxUDxUUq9zi2tOIl+6
ALSn7l1sKMxPVb0fohyyuRzRspt/TYmvV6oorF8J62I=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
61r5RjlUpp0Sx9otiMiZNQFewfAHPXct4XNb20i2Qy085lteyha1wknNg1lweS6E
9a04f079-9840-4286-ab92-e65be0885f95
5181942b9ebc31ce68dacb56c16fd79f
1df99396a8d31184ecc33b21b338d142
cc2751449a350f668590264ed76692694a80308a
470fa2b4ae81cd56ecbcda9735803434cec591fa
lXWwWv5JK/+sPkAKl3c1KDv4Hvk1BPLRteoZBxJagTzyJxEU8SumoR58fR6LdW3i
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
MDEyMzQ1Njc4OUFCQ0RFRjAxMjM0NTY3ODlBQkNERUY=
TPzVsbfBdc04crERn4ev6bozRLSTEZrNgI+oWWW2p5k=
x244HDzWeCJXpaVmJz6ZDJ8SomiOjqvEXNm93LF/UprnziaRy0GWl7kRtW31unI7

POSSIBLE SECRETS
pFqkMlhSSaQ2eu0bhmIAWpk2TrQlPQpWFME4RoGI1ncpKXXKi44CuFe8cYNKvx1r
xLOAO7msIR4UFUyldUn5stL2wwbLdISu2CSlTLg4f6Q=
tfuuP59pzWN+H8zv1geT3jADiBKBGMQRjmCPoIvL5f45Lvl5qgJ0PgBqZF4WPnQj
0ed6021be1a78f9233e7f8206b608c68
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
b0nnYr5Y43sLp9uCG6eLzyBhSsauFEDPWpaZrhJ4ttc=
BkxOKZDOMH8NUFJEmpCq1X+PtIP0kLI1Ua0ujwsrkUE=
26320202e140f5c4ac9ff757ed1368a7
86197cebc59f71fbc12214f2a5780326
MbAcGuLi+XGl3MsgqAiQYLikemL120ZFxn+dIhaD+rHWJuTeO/M8+1c58cczHjCs
3e2ef083c39ea48f71dd557121824280
hDi2yHM1WBnaBo8xfxWY0dwLv3vkmI37udU/dWBh2W+Ynkfo3oZQp4Q+03pBto4q
sK9i540XcONymgaiZVMKYXr1VbNcwMhjwo2LFhhSCFg=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9
c56fb7d591ba6704df047fd98f535372fea00211
7870a762b4839167d1971cbfd2559a98
qzPpYppPAZhPHZoGToPEj4gLCkf1GlGnviIXlGI2ic/egZu+qobDN2aG3wSrxpBD
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
5967b44948d2ac0c0f76514065562865
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
xYPp9mA9NiiAUtoW1mf06CeivM3OQ2f/EXuQXBQemfo=
3QFFvrLAbfvZBnCmYb/H5Zm44EsMhBJStIcWOORiyIo=

POSSIBLE SECRETS
ZCuJ2BZ9pjX66HItj5rJVOE3CFRvMlTjLwpTXK/hjirliOmVxPsb2SejOT7YbM4P
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
aC7c3pDenGsdb0eFildzKOBrhobw8fKkmd52rTlBEKM=
0c14e7400baf7014368a26628922227b
64c4efbe8d13073453ebdb52174636aa
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: SoundCloud: Play Music & Songs

Score: 4.6829915 **Installs:** 100,000,000+ **Price:** 0 **Android Version Support:** **Category:** Music & Audio **Play Store URL:** com.soundcloud.android

Developer Details: SoundCloud, 5736420085696151391, Rheinsberger Str. 76, 10115 Berlin, Germany, http://soundcloud.com/mobile, contact@soundcloud.com,

Release Date: Dec 21, 2010 **Privacy Policy:** Privacy link

Description:

What’s next in music is first on SoundCloud. Be the first to find new music. Discover trending artists, play songs and share your favorite playlists. Access the world’s largest music discovery platform - That’s 300M+ tracks from 30M+ artists in 193 countries Discover new and trending music, picked just for you - Play curated mixes and playlists based on the songs you love Find exclusive music on SoundCloud - Play songs, DJ sets and remixes you can’t find on any other streaming platform Grow your music collection - Find and save trending hits, underground remixes, deep cuts and more. - Build playlists with your favorite songs. Find and connect with your music community - Follow your favorite artists and connect with music fans directly and discover their playlists. - Like, Repost and comment on any track, directly in the music player. - Share songs and trending playlists on the app and social media. Upload your own tracks - Upload your own music directly on the app to tap into a global fanbase of millions and start trending. Help independent artists get paid - Your fan-powered streams puts money in the pockets of the artists YOU want to support. Enjoy free music streaming with SoundCloud FREE, or level up with SoundCloud Go or SoundCloud Go+ to remove ads, play songs offline and more premium features. SOUNDCLOUD FREE: - Play music from independent and established artists (with ads). - Listen to albums and playlists with unlimited skips. - Stream music on your Wear OS smartwatch. SOUNDCLOUD Go: - Listen without ads - Save tracks to listen offline — Play your favorite songs and playlists anytime, anywhere - Support your favorite independent artists through Fan-Powered Royalties SOUNDCLOUD Go+: - Unlock premium Go+ tracks - Access high-quality audio streaming - Upgrade your DJ sets with exclusive app integrations - Listen without ads - Save tracks to listen offline — hear your favorite songs and playlists anytime, anywhere - Support your favorite independent artists through Fan-Powered Royalties SoundCloud Go+ gives you offline and ad-free listening to everything from mainstream songs to trending DJ sets and remixes. Need help? Get in touch: https://soundcloudcommunity.com https://help.soundcloud.com https://twitter.com/SCsupport SoundCloud is available in English, Brazilian Portuguese, Dutch, French, German, Italian and Spanish. Privacy Policy: https://soundcloud.com/pages/privacy Terms of Use: https://soundcloud.com/terms-of-use

Report Generated by - MobSF v3.9.3 Beta

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.