ANDROID STATIC ANALYSIS REPORT

app_icon

Habitica (3.2.3)

File Name:	com.habitrpg.android.habitica_2934_apps.evozi.com.apk

Package Name:	com.habitrpg.android.habitica
Scan Date:	Dec. 2, 2024, 7:29 p.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
6	21	3	1	0

FILE INFORMATION

File Name: com.habitrpg.android.habitica_2934_apps.evozi.com.apk
Size: 19.53MB
MD5: bef5e622b6e8fff25e6cec4249ddefde
SHA1: aa95e97558a3021a6940f07f6d9f879adafb57a5
SHA256: 8e9eeae37cc8cc17c054a1753a9feef53db18b06936ad3939833d5c323c906b7

APP INFORMATION

App Name: Habitica
Package Name: com.habitrpg.android.habitica
Main Activity: com.habitrpg.android.habitica.ui.activities.MainActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 3.2.3
Android Version Code: 2934

APP COMPONENTS

Activities: 30

Services: 11
Receivers: 12
Providers: 5
Exported Activities: 5
Exported Services: 1
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: O=HabitRPG
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-06-18 22:16:25+00:00
Valid To: 2040-06-11 22:16:25+00:00
Issuer: O=HabitRPG
Serial Number: 0x1bca5e2e
Hash Algorithm: sha256
md5: 6a146c16792fe181cef9ca1eee2b14a8
sha1: 00ec9085559c85957e76ae8d271e6dbfce7a773e
sha256: 0843e6e0a64db0534e919d196e42d53f4f5cdcc462a4e83577beb469fdcb94b4
sha512: 7d55285de83673e946c7dc7bc2cfc595abe378d58bba4b14e848789cacfe08fa7b2d88cee938fc8983663ca73be86263f388ee6531b6519c646e5a0f0ce67d17
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5a0e3d4a96537ce96fa361fa9c4d8910b562f3ea20a3b24fcdf11fa401bf1490
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.habitrpg.android.habitica.ui.activities.MainActivity	Schemes: https://, http://, Hosts: habitica.com, Paths: /inventory/equipment, /tasks, /, /party, /party/quest, /user/stats, /tavern, /groups/myGuilds, /challenges/myChallenges, /challenges/findChallenges, /inventory/items, /inventory/stable, /static/faq, Path Prefixes: /user/tasks/, /groups/guild/, /challenges/, Path Patterns: /,
com.habitrpg.android.habitica.ui.activities.PrefsActivity	Schemes: https://, Hosts: habitica.com, Path Patterns: /settings/.*,
com.habitrpg.android.habitica.ui.activities.FullProfileActivity	Schemes: https://, Hosts: habitica.com, Path Patterns: /profile/.*,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.habitrpg.android.habitica,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	10.0.0.107	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

🔍 MANIFEST ANALYSIS

HIGH: **4** | WARNING: **14** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	App Link assetlinks.json file not found [android:name=com.habitrpg.android.habitica.ui.activities.MainActivity] [android:host=https://habitica.com]	high	App Link asset verification URL (https://habitica.com/.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.
5	App Link assetlinks.json file not found [android:name=com.habitrpg.android.habitica.ui.activities.PrefsActivity] [android:host=https://habitica.com]	high	App Link asset verification URL (https://habitica.com/.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	Activity (com.habitrpg.android.habitica.ui.activities.PrefsActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
7	App Link assetlinks.json file not found [android:name=com.habitrpg.android.habitica.ui.activities.FullProfileActivity] [android:host=https://habitica.com]	high	App Link asset verification URL (https://habitica.com/.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
8	Activity (com.habitrpg.android.habitica.ui.activities.FullProfileActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
9	Broadcast Receiver (com.habitrpg.android.habitica.receivers.TaskReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.habitrpg.android.habitica.receivers.TaskAlarmBootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [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.
11	Activity (com.habitrpg.android.habitica.ui.activities.AddTaskWidgetActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
12	Activity (com.habitrpg.android.habitica.ui.activities.HabitButtonWidgetActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
13	Broadcast Receiver (com.habitrpg.android.habitica.widget.AvatarStatsWidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Broadcast Receiver (com.habitrpg.android.habitica.widget.DailiesWidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Broadcast Receiver (com.habitrpg.android.habitica.widget.TodoListWidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
16	Broadcast Receiver (com.habitrpg.android.habitica.widget.HabitButtonWidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
17	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.
18	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.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **0** | WARNING: **4** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amplitude/api/g.java com/habitrpg/android/habitica/HabiticaBaseApplication.java com/habitrpg/android/habitica/helpers/MainNavigationController.java com/habitrpg/android/habitica/helpers/SignInWebViewClient.java com/habitrpg/android/habitica/helpers/SignInWebViewDialogFragment.java com/habitrpg/android/habitica/ui/AvatarView.java com/habitrpg/android/habitica/ui/activities/MainActivity.java com/habitrpg/android/habitica/ui/views/DragLinearLayout.java e/a/k/a/a.java e/a/o/g.java e/f/b/k/f.java e/h/e/c.java e/h/e/e.java e/h/e/f.java e/h/e/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	e/h/e/g.java e/h/e/j.java e/h/e/k.java e/h/i/c.java e/h/j/b.java e/h/k/b.java e/h/k/d0.java e/h/k/e0/c.java e/h/k/g.java e/h/k/i.java e/h/k/u.java e/h/k/v.java e/h/k/y.java e/j/a/c.java e/o/a/a.java e/p/a/b.java e/p/b/c.java e/q/a/a.java e/t/i0.java e/t/y.java e/u/a/a/i.java f/b/a/a/a.java f/c/a/a/i/v/a.java f/c/a/c/b0/g.java f/c/a/c/m/h.java f/c/a/c/o/a.java f/c/a/c/y/d.java f/c/a/c/z/b.java f/d/a/a/d.java i/a/a/d.java i/a/a/x/d.java i/a/a/x/v/b.java i/a/a/x/x/b.java org/greenrobot/eventbus/f.java org/solovyev/android/checkout/o.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/habitrpg/android/habitica/BuildConfig.java com/habitrpg/android/habitica/HabiticaPurchaseVerifier.java com/habitrpg/android/habitica/helpers/KeyHelper.java com/habitrpg/android/habitica/helpers/SignInWebViewDialogFragment.java com/habitrpg/android/habitica/helpers/SignInWithAppleResult.java com/habitrpg/android/habitica/helpers/TaskAlarmManager.java com/habitrpg/android/habitica/helpers/notifications/PushNotificationManager.java com/habitrpg/android/habitica/ui/activities/ChallengeFormActivity.java com/habitrpg/android/habitica/ui/activities/GiftGemsActivityArgs.java com/habitrpg/android/habitica/ui/activities/GiftSubscriptionActivityArgs.java com/habitrpg/android/habitica/ui/activities/GroupInviteActivity.java com/habitrpg/android/habitica/ui/activities/TaskFormActivity.java com/habitrpg/android/habitica/ui/fragments/inventory/items/ItemRecyclerFragment.java com/habitrpg/android/habitica/ui/fragments/inventory/shops/ShopFragment.java com/habitrpg/android/habitica/ui/fragments/inventory/stable/MountDetailRecyclerFragment.java com/habitrpg/android/habitica/ui/fragments/inventory/stable/PetDetailRecyclerFragment.java com/habitrpg/android/habitica/ui/fragments/inventory/stable/StableRecyclerFragment.java com/habitrpg/android/habitica/ui/fragments/social/InboxMessageListFragmentArgs.java com/habitrpg/android/habitica/ui/fragments/social/InboxOverviewFragmentDirections.java com/habitrpg/android/habitica/ui/fragments/tasks/TaskRecyclerViewFragment.java org/solovyev/android/checkout/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/habitrpg/android/habitica/receivers/NotificationPublisher.java com/habitrpg/android/habitica/ui/fragments/setup/AvatarSetupFragment.java com/habitrpg/android/habitica/ui/views/login/LoginBackgroundView.java f/e/a/d.java f/e/a/e/a.java f/e/a/e/b.java f/e/a/e/c.java f/e/a/e/d.java
4	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/habitrpg/android/habitica/ui/activities/FullProfileActivity.java com/habitrpg/android/habitica/ui/fragments/preferences/APIPreferenceFragment.java com/habitrpg/android/habitica/ui/fragments/preferences/AuthenticationPreferenceFragment.java com/habitrpg/android/habitica/ui/fragments/social/ChatFragment.java com/habitrpg/android/habitica/ui/fragments/social/InboxMessageListFragment.java com/habitrpg/android/habitica/ui/fragments/social/party/NoPartyFragmentFragment.java
5	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	com/amplitude/api/j.java f/c/a/a/i/x/j/b0.java f/c/a/a/i/x/j/f0.java f/c/a/a/i/x/j/h0.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/habitrpg/android/habitica/data/implementation/ApiClientImpl.java com/habitrpg/android/habitica/modules/ApiModule.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/habitrpg/android/habitica/helpers/SoundFileLoader.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__vsprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__vsprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

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

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

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__vsprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64-v8a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	x86_64/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	x86_64/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__vsprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86_64/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86_64/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

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

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

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	x86/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/habitrpg/android/habitica/receivers/LocalNotificationActionReceiver.java com/habitrpg/android/habitica/receivers/TaskReceiver.java com/habitrpg/android/habitica/ui/activities/ChallengeFormActivity.java com/habitrpg/android/habitica/ui/activities/FullProfileActivity.java com/habitrpg/android/habitica/ui/activities/GroupFormActivity.java com/habitrpg/android/habitica/ui/activities/MaintenanceActivity.java com/habitrpg/android/habitica/ui/activities/TaskFormActivity.java com/habitrpg/android/habitica/ui/fragments/social/guilds/GuildDetailFragment.java com/habitrpg/android/habitica/ui/fragments/social/guilds/GuildFragment.java com/habitrpg/android/habitica/ui/fragments/social/party/NoPartyFragmentFragment.java com/habitrpg/android/habitica/ui/fragments/social/party/PartyFragment.java
00013	Read file and put it into a stream	file	com/getkeepsafe/relinker/f/i.java e/h/e/e.java e/h/e/k.java i/a/a/x/u/a.java okio/r.java
00022	Open a file from given absolute path of the file	file	com/getkeepsafe/relinker/c.java com/habitrpg/android/habitica/HabiticaBaseApplication.java io/realm/d0.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java
00025	Monitor the general action to be performed	reflection	com/habitrpg/android/habitica/ui/activities/TaskFormActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/habitrpg/android/habitica/ui/activities/MaintenanceActivity.java com/habitrpg/android/habitica/ui/fragments/AboutFragment.java com/habitrpg/android/habitica/ui/fragments/social/challenges/ChallengeDetailFragment$showEndChallengeDialog$1.java com/habitrpg/android/habitica/ui/fragments/social/guilds/GuildOverviewFragment$showCreationDialog$1.java com/habitrpg/android/habitica/ui/fragments/support/BugFixFragment.java com/habitrpg/android/habitica/ui/fragments/support/SupportMainFragment.java com/habitrpg/android/habitica/ui/views/subscriptions/SubscriptionDetailsView.java com/habitrpg/android/habitica/widget/TaskListWidgetProvider.java i/a/a/d.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/habitrpg/android/habitica/ui/fragments/AboutFragment.java com/habitrpg/android/habitica/ui/fragments/support/BugFixFragment.java com/habitrpg/android/habitica/widget/TaskListWidgetProvider.java
00096	Connect to a URL and set request method	command network	com/habitrpg/android/habitica/helpers/DeviceName.java
00123	Save the response to JSON after connecting to the remote server	network command	com/habitrpg/android/habitica/helpers/DeviceName.java
00089	Connect to a URL and receive input stream from the server	command network	com/amplitude/api/h.java com/habitrpg/android/habitica/helpers/DeviceName.java i/a/a/x/w/a.java
00030	Connect to the remote server through the given URL	network	com/habitrpg/android/habitica/helpers/DeviceName.java i/a/a/x/w/a.java
00109	Connect to a URL and get the response code	network command	com/amplitude/api/h.java com/habitrpg/android/habitica/helpers/DeviceName.java i/a/a/x/w/a.java
00012	Read data and put it into a buffer stream	file	i/a/a/x/u/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	com/habitrpg/android/habitica/receivers/LocalNotificationActionReceiver.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/j.java
00004	Get filename and put it to JSON object	file collection	com/amplitude/api/j.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/f.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	e/h/k/e0/c.java
00036	Get resource file from res/raw directory	reflection	com/habitrpg/android/habitica/widget/TaskListWidgetProvider.java i/a/a/d.java
00078	Get the network operator name	collection telephony	com/amplitude/api/l.java
00137	Get last known location of the device	location collection	com/amplitude/api/l.java
00115	Get last known location of the device	collection location	com/amplitude/api/l.java
00132	Query The ISO country code	telephony collection	com/amplitude/api/l.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://habitica-android-production.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1035232791481/namespaces/firebase:fetch?key=AIzaSyAzQXmicLxjCSGAFHRre4OB4KQ_J0yIrNE is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'activePromo': '_fall', 'customMenu': '[{"key":"user","items":["skills","stats","achievements"]},{"key":"shops","items":["market","questShop","customizationShop","seasonalShop","timeTravelersShop"]},{"key":"inventory","items":["customizeAvatar","equipment","items","stable","gems","subscription"]},{"key":"social","items":["party","challenges"]},{"key":"about","items":["news","support","about"]}]', 'disableIntroSlides': 'false', 'enableAdventureGuide': 'true', 'enableArmoireSubs': 'true', 'enableCustomizationShop': 'true', 'enableFaintSubs': 'true', 'enableGiftOneGetOne': 'false', 'enableLocalChanges': 'true', 'enableLocalTaskScoring': 'false', 'enablePushMentions': 'true', 'enableReviewPrompt': 'true', 'enableTaskDisplayMode': 'false', 'enableTeamBoards': 'false', 'enableUsernameAutocomplete': 'false', 'feedbackURL': 'https://docs.google.com/forms/d/e/1FAIpQLScPhrwq_7P1C6PTrI3lbvTsvqGyTNnGzp1ugi1Ml0PFee_p5g/viewform', 'flipAddTaskBehaviour': 'true', 'hideFacebook': 'true', 'hideGuilds': 'true', 'hideTavern': 'true', 'insufficientGemPurchase': 'true', 'insufficientGemPurchaseAdjust': 'false', 'knownIssues': '[{"title":"New shop isn\'t showing in the menu","text":"It can take some time for the new configuration to roll out to everyone! You can check the About section from the menu to be sure you\'re on version 4.4 that has proper support for all the new features. If you\'re on that version, give it about an hour. You can also try uninstalling and reinstalling to get the changes faster."},{"title":"Task reminders aren’t showing","text":"In order to receive task reminders more reliably, we recommend allowing Habitica unrestricted battery settings to be sure reminders aren’t delayed when you aren’t using the app. You can change this from your device’s Settings app under Apps > Habitica > Battery Usage. Some devices may refer to this setting as ‘Ignore battery optimization’."},{"title":"Dailies not resetting","text":"We’re currently investigating the cause for this issue. If this happens to you, try closing and reopening the app, logging out and back in, going to Settings and tapping \'Reload Content\', or logging in to the [Habitica Website](https://habitica.com) may force a reset. If none of the above helps, please let us know by tapping the ‘Report a Bug’ button on the previous screen."},{"title":"Lost HP, Gold, or level to a bug","text":"If something happened to damage your avatar due to a bug, you can fix some of the values by going to Menu > Settings > My Account > Fix Character Values."}]', 'lastVersionCode': '2582', 'lastVersionNumber': '3.0.1', 'maxChatLength': '3000', 'moveAdventureGuide': 'true', 'noPartyLinkPartyGuild': 'true', 'prodHost': 'habitica.com', 'raiseShops': 'true', 'randomizeAvatar': 'false', 'reorderMenu': 'true', 'shopSpriteSuffix': '_spring', 'showSubscriptionBanner': 'false', 'showTaskGraphs': 'false', 'spriteSubstitutions': '{}', 'stableName': 'Stable', 'subChangeDate': '2024-11-19T18:00:00Z', 'supportEmail': 'admin@habitica.com', 'surveyURL': 'https://docs.google.com/forms/d/e/1FAIpQLSfAPPdCC6LT1LZFJGhabb1Jt6YwyRAJGd80bE1T7hvVPyMHoA/viewform?usp=pp_url&entry.273783256=USER_ID'}, 'state': 'UPDATE', 'templateVersion': '247'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	2/44	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
twitter.com	ok	**IP:** 104.244.42.129 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
regionconfig.amplitude.com	ok	**IP:** 54.192.51.8 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.23.96.16 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
habitica.com	ok	**IP:** 146.148.62.68 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
api2.amplitude.com	ok	**IP:** 100.20.160.207 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.32.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
realm.io	ok	**IP:** 3.162.3.88 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
habitrpg-delta.herokuapp.com	ok	**IP:** 54.205.8.205 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
s3.amazonaws.com	ok	**IP:** 16.15.216.117 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.409912 **Longitude:** -122.160400 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
habitica-assets.s3.amazonaws.com	ok	**IP:** 3.5.27.80 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
habitica-android-production.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.69.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
raw.githubusercontent.com	ok	**IP:** 185.199.109.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
□□□□□□□□□□□□admin@habitica.com□□□□□□□ admin@habitica.com□ admin@habitica.com □□□□□□□□□□□□admin@habitica.com □□□□□□□□□□□□admin@habitica.com	Android String Resource
help@realm.io	lib/arm64-v8a/librealm-jni.so
help@realm.io	lib/x86_64/librealm-jni.so
help@realm.io	lib/armeabi-v7a/librealm-jni.so
help@realm.io	lib/x86/librealm-jni.so
help@realm.io	apktool_out/lib/arm64-v8a/librealm-jni.so
help@realm.io	apktool_out/lib/x86_64/librealm-jni.so
help@realm.io	apktool_out/lib/armeabi-v7a/librealm-jni.so

EMAIL	FILE
help@realm.io	apktool_out/lib/x86/librealm-jni.so

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Lozinka"
"password" : "Şifre"
"could_not_find_user" : "□□□□□□□□□□□□"
"password" : "סיסמה"

POSSIBLE SECRETS
"password" : "Contraseña"
"block_user" : "□□□□□□□□□□□"
"username" : "Benutzername"
"enter_recipient_username" : "□□□□□□@□□□"
"username" : "□□□"
"add_local_authentication" : "□□□□□□□□□□□"
"username" : "□□□"
"delete_oauth_account_description" : "□□"
"delete_oauth_account_description" : "□□"
"SP_APIToken" : "APIToken"
"username" : "□□□□□"
"password" : "Парола"
"email_username" : "□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□"
"password" : "Hasło"

POSSIBLE SECRETS
"copy_username" : "□□□□□"
"google_api_key" : "AIzaSyAzQXmicLxjCSGAFHRre4OB4KQ_J0yIrNE"
"invited_to_private_guild" : "□□□□□□□□□□%1$s□□□□□□□□□"
"password" : "□□"
"unblock_user" : "□□□□□□□□□□□□□□"
"google_crash_reporting_api_key" : "AIzaSyAzQXmicLxjCSGAFHRre4OB4KQ_J0yIrNE"
"invited_to_private_guild" : "□□□□□□□□□□□□<b>%1$s</b>"
"add_local_authentication" : "□□□□□□□"
"SP_APIToken_title" : "API□□"
"password" : "Senha"
"block_user" : "□□□□□"
"email_username" : "□□□□□□□□□□□□□□□"
"could_not_find_user" : "□□□□□"
"password" : "Palavra-passe"
"username" : "Gebruikersnaam"
"password" : "Passwort"

POSSIBLE SECRETS
"SP_APIToken_title" : "API-Token"
"password" : "□□"
"password" : "□□"
"could_not_find_user" : "□□□□□"
"unblock_user" : "□□□□□□□"
"email_username" : "□□□□□□□□"
"invited_to_private_guild" : "□□□□□<b>%1$s</b>□□□□"
"copy_username" : "□□□□□"
"SP_APIToken_title" : "API-token"
"password" : "Password"
"username" : "□□□□□"
"add_local_authentication" : "□□□□□□□"
"password" : "□□□□□"
"copy_username" : "□□□□□□□□□□□□"
"username" : "Username"
"password" : "Slaptažodis"

POSSIBLE SECRETS
"fabric_key" : "2eb3b3edb3b0f4722d37d649a5af366656e46ddd"
"firebase_database_url" : "https://habitica-android-production.firebaseio.com"
"SP_APIToken_summary" : "□□API□□"
"password" : "Пароль"
"password" : "Wachtwoord"
4b23d656-025d-41bd-b61e-dd7f58af1899
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
cc2751449a350f668590264ed76692694a80308a
9b8f518b086098de3d77736f9458a3d2f6f95a37
f2db2a7f-13c5-454d-b3ee-ea1f5089e601
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
5481ccf3-5d2d-48a9-a871-70a7380cee5a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: Habitica: Gamify Your Tasks

Score: 4.733207 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Productivity **Play Store URL:** com.habitrpg.android.habitica

Developer Details: HabitRPG, Inc., 7023585019856140116, 11870 Santa Monica Blvd. Suite 106-577 Los Angeles, CA 90025, https://habitica.com, mobile@habitica.com,

Release Date: Dec 10, 2015 **Privacy Policy:** Privacy link

Description:

Habitica is a free habit-building and productivity app that uses retro RPG elements to gamify your tasks and goals. Use Habitica to help with ADHD, self care, New Year’s resolutions, household chores, work tasks, creative projects, fitness goals, back-to-school routines, and more! How it works: Create an avatar then add tasks, chores, or goals you’d like to work on. When you do something in real life, check it off in the app and receive gold, experience, and items that can be used in-game! Features: • Automatically repeating tasks scheduled for your daily, weekly, or monthly routines • Flexible habit tracker for tasks you want to do multiple times a day or only once in awhile • Traditional to do list for tasks that only need to be done once • Color coded tasks and streak counters help you see how you’re doing at a glance • Leveling system to visualize your overall progress • Tons of collectable gear and pets to suit your personal style • Inclusive avatar customizations: wheelchairs, hair styles, skin tones, and more • Regular content releases and seasonal events to keep things fresh • Parties let you team up with friends for extra accountability and battle fierce foes by completing tasks • Challenges offer shared task lists you can add to your personal tasks • Reminders and widgets to help keep you on track • Customizable color themes with dark and light mode • Syncing across devices Want even more flexibility to take your tasks on the go? We have a Wear OS app on the watch! Wear OS features: • View, create, and complete Habits, Dailies, and To do’s • Receive rewards for your efforts with experience, food, eggs, and potions • Track your stats with dynamic progress bars • Show off your stunning pixel avatar on the watch face — Run by a small team, Habitica is an open-source app made better by contributors who create translations, bug fixes, and more. If you’d like to contribute, you can check out our GitHub or reach out for more information! We highly value community, privacy, and transparency. Rest assured, your tasks remain private and we never sell your personal data to third parties. Questions or feedback? Feel free to reach us at admin@habitica.com! If you’re enjoying Habitica, we’d be thrilled if you leave us a review. Start your journey towards productivity, download Habitica now!

SCAN LOGS

Timestamp	Event	Error
2024-12-02 19:29:25	Generating Hashes	OK

2024-12-02 19:29:25	Extracting APK	OK
2024-12-02 19:29:25	Unzipping	OK
2024-12-02 19:29:25	Getting Hardcoded Certificates/Keystores	OK
2024-12-02 19:29:25	Parsing APK with androguard	OK
2024-12-02 19:29:27	Parsing AndroidManifest.xml	OK
2024-12-02 19:29:27	Extracting Manifest Data	OK
2024-12-02 19:29:27	Manifest Analysis Started	OK
2024-12-02 19:29:28	Reading Network Security config from network_security_config.xml	OK
2024-12-02 19:29:28	Parsing Network Security config	OK
2024-12-02 19:29:28	Performing Static Analysis on: Habitica (com.habitrpg.android.habitica)	OK
2024-12-02 19:29:28	Fetching Details from Play Store: com.habitrpg.android.habitica	OK

2024-12-02 19:29:29	Checking for Malware Permissions	OK
2024-12-02 19:29:29	Fetching icon path	OK
2024-12-02 19:29:29	Library Binary Analysis Started	OK
2024-12-02 19:29:29	Analyzing lib/arm64-v8a/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing lib/arm64-v8a/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing lib/arm64-v8a/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing lib/arm64-v8a/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing lib/arm64-v8a/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing lib/x86_64/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing lib/x86_64/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing lib/x86_64/librealm-jni.so	OK

2024-12-02 19:29:29	Analyzing lib/x86_64/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing lib/x86_64/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing lib/armeabi-v7a/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing lib/armeabi-v7a/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing lib/armeabi-v7a/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing lib/armeabi-v7a/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing lib/armeabi-v7a/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing lib/x86/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing lib/x86/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing lib/x86/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing lib/x86/libgifimage.so	OK

2024-12-02 19:29:29	Analyzing lib/x86/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/arm64-v8a/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/arm64-v8a/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/arm64-v8a/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/arm64-v8a/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/arm64-v8a/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86_64/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86_64/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86_64/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86_64/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86_64/libnative-filters.so	OK

2024-12-02 19:29:29	Analyzing apktool_out/lib/armeabi-v7a/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/armeabi-v7a/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/armeabi-v7a/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/armeabi-v7a/libnative-filters.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86/libnative-imagetranscoder.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86/libimagepipeline.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86/librealm-jni.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86/libgifimage.so	OK
2024-12-02 19:29:29	Analyzing apktool_out/lib/x86/libnative-filters.so	OK
2024-12-02 19:29:29	Reading Code Signing Certificate	OK

2024-12-02 19:29:30	Running APKiD 2.1.5	OK
2024-12-02 19:29:33	Updating Trackers Database....	OK
2024-12-02 19:29:33	Detecting Trackers	OK
2024-12-02 19:29:34	Decompiling APK to Java with JADX	OK
2024-12-02 19:29:46	Converting DEX to Smali	OK
2024-12-02 19:29:46	Code Analysis Started on - java_source	OK
2024-12-02 19:29:47	Android SBOM Analysis Completed	OK
2024-12-02 19:29:51	Android SAST Completed	OK
2024-12-02 19:29:51	Android API Analysis Started	OK
2024-12-02 19:29:52	Android API Analysis Completed	OK
2024-12-02 19:29:53	Android Permission Mapping Started	OK

2024-12-02 19:29:55	Android Permission Mapping Completed	OK
2024-12-02 19:29:55	Android Behaviour Analysis Started	OK
2024-12-02 19:29:59	Android Behaviour Analysis Completed	OK
2024-12-02 19:29:59	Extracting Emails and URLs from Source Code	OK
2024-12-02 19:30:00	Email and URL Extraction Completed	OK
2024-12-02 19:30:00	Extracting String data from APK	OK
2024-12-02 19:30:00	Extracting String data from SO	OK
2024-12-02 19:30:00	Extracting String data from Code	OK
2024-12-02 19:30:00	Extracting String values and entropies from Code	OK
2024-12-02 19:30:02	Performing Malware check on extracted domains	OK
2024-12-02 19:30:03	Saving to Database	OK

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.