ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 MyNetDiary (9.1.6)

File Name:	com.fourtechnologies.mynetdiary.ad_144690.apk
Package Name:	com.fourtechnologies.mynetdiary.ad
Scan Date:	Aug. 29, 2025, 10:31 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	30	3	2	1

FILE INFORMATION

File Name: com.fourtechnologies.mynetdiary.ad_144690.apk
Size: 147.63MB
MD5: 9a0796d719c9ed1cb0e8ad62b194f091
SHA1: 22932eea50606ba82457dc54e8d601800dbc29a0
SHA256: f9bbe2b5dc0cbd9ee132b8f4af4ad53be170c71ec654f3f6528cf4548e90768e

APP INFORMATION

App Name: MyNetDiary
Package Name: com.fourtechnologies.mynetdiary.ad
Main Activity: com.mynetdiary.auth.AuthActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 9.1.6

Android Version Code: 144690

■■ APP COMPONENTS

Activities: 32
Services: 21
Receivers: 24
Providers: 7
Exported Activities: 10
Exported Services: 4
Exported Receivers: 4
Exported Providers: 0

✺ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=NJ, L=Cherry Hill, O=4Technologies Corporation, OU=MyNetDiary, CN=MyNetDiary
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-09-17 16:40:17+00:00
Valid To: 2038-02-02 16:40:17+00:00
Issuer: C=US, ST=NJ, L=Cherry Hill, O=4Technologies Corporation, OU=MyNetDiary, CN=MyNetDiary
Serial Number: 0x4c9399f1
Hash Algorithm: md5
md5: 21fe77ebbbb1e07ce686b7b4915591cd
sha1: d08c47cc57c663f075055216945808065218c6e8
sha256: 9431fd9985c87bf1e5a05c3fd430ba0796dee72f837cda9d974438bc119d5ecb
sha512: de7a6e108cf84a5eee16b88b00daaad48bbd3d5ff7f015e00f762829f78b9d9a2a6d3c3b3c9250cb39f93dbb774594c4ba8bf79e5044498cfc3a12729beef2e1
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 89a098dcd686f0ed00878a51b576cb35afebdbe29bcec0770300410be8e14767
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.health.READ_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_RESTING_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_RESTING_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.READ_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BONE_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BONE_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_DISTANCE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_FLOORS_CLIMBED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_SLEEP	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_HYDRATION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.WRITE_HYDRATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_NUTRITION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_ACTIVE_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_TOTAL_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.fourtechnologies.mynetdiary.ad.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
9a0796d719c9ed1cb0e8ad62b194f091.apk	**FINDINGS** / **DETAILS** Anti-VM Code — possible VM check
classes.dex	**FINDINGS** / **DETAILS** Anti-VM Code — Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / Build.HARDWARE check Compiler — r8
classes2.dex	**FINDINGS** / **DETAILS** Anti-VM Code — Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / Build.HARDWARE check / SIM operator check / network operator name check Compiler — r8 without marker (suspicious)

FILE	DETAILS
classes3.dex	<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.BOARD check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes5.dex	<table><tr><td>**FINDINGS**</td><td>**DETAILS**</td></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check Build.BOARD check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes6.dex	<table><tr><td>**FINDINGS**</td><td>**DETAILS**</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mynetdiary.auth.AuthActivity	Schemes: http://, https://, mnd://, Hosts: www.mynetdiary.com, mnd, Paths: /shareRecipe.do, /inviteProfessional.do, /inviteClient.do, /weeklyEmailTap.do, /google_assistant_log_food, Path Prefixes: /community/friendinvitations, /community/groupinvitations, /community/groups, /community/posts,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.fourtechnologies.mynetdiary.ad,

ACTIVITY	INTENT
com.mynetdiary.wear.mobile.ui.StartFromWearActivity	Schemes: mnd://, Hosts: mobile, Paths: /free/screen/main,
com.mynetdiary.account.passwordreset.ResetPasswordActivity	Schemes: http://, https://, Hosts: www.mynetdiary.com, Paths: /resetPasswordPage.do,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

📇 CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

🔍 MANIFEST ANALYSIS

HIGH: **1** | WARNING: **19** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Activity (com.mynetdiary.ui.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	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.
5	Activity (com.mynetdiary.wear.mobile.ui.StartFromWearActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (com.mynetdiary.wear.mobile.service.WearAppRequestsListenerService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (com.mynetdiary.account.passwordreset.ResetPasswordActivity) 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.
8	Activity (com.mynetdiary.feature.integrations.healthconnect.ui.HealthConnectPermissionsRationaleActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity-Alias (com.mynetdiary.feature.integrations.healthconnect.HealthConnectPermissionsRationaleActivityApi34) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Broadcast Receiver (com.mynetdiary.feature.fasting.presentation.widget.service.FastingWidgetBootReceiver) 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.
11	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
13	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.
14	Activity (com.canhub.cropper.CropImageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

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

NO	ISSUE	SEVERITY	DESCRIPTION
17	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.
18	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
19	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

</> CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a8/a.java aa0/c.java ab/h.java ad/h.java ae/f.java ae/h.java ae/i.java ae/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ao0/l0.java au/ao.java au/y0.java b4/a.java bi0/g.java bk0/k.java bm/h.java bq/d.java bu/w.java bv/k.java bx/a.java c30/j0.java c30/k.java c30/p.java ca0/c.java cb/a.java cj0/f.java cj0/l.java ck0/f.java ck0/g.java com/airbnb/lottie/LottieAnimationView.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/a0.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/b0.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/e0.java com/bumptech/glide/load/resource/bitmap/f.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				java com/bumptech/glide/load/resource/bitmap/o.java com/bumptech/glide/load/resource/bitmap/p.java com/bumptech/glide/load/resource/bitmap/t.java com/bumptech/glide/request/SingleRequest.java com/canhub/cropper/CropImageActivity.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/davemorrissey/labs/subscaleview/decoder/SkiaPooledImageRegionDecoder.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/listener/a.java com/github/panpf/zoomimage/util/a.java com/mynetdiary/account/backup/b.java com/mynetdiary/account/credential/ChangeCredentialViewModel.java com/mynetdiary/account/passwordreset/a.java com/mynetdiary/account/signin/SignInViewModel.java com/mynetdiary/account/signin/b.java com/mynetdiary/account/signup/SignUpViewModel.java com/mynetdiary/account/signup/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mynetdiary/account/signup/e.java com/mynetdiary/auth/c.java com/mynetdiary/billing/a.java com/mynetdiary/bridgetolegacy/AccountProxyFragment.java com/mynetdiary/bridgetolegacy/CommunityExternalNavigatorImpl.java com/mynetdiary/common/analytics/impl/manalytics/d.java com/mynetdiary/common/analytics/impl/mobileactionlog/a.java com/mynetdiary/common/analytics/impl/mobileactionlog/b.java com/mynetdiary/common/android/util/DebugLog.java com/mynetdiary/common/images/ImagePicker.java com/mynetdiary/common/images/PhotoTaker.java com/mynetdiary/common/images/cropper/a.java com/mynetdiary/community/CommunityQuickActionsService.java com/mynetdiary/community/common/view/BlurryEdgesImageView.java com/mynetdiary/community/common/view/DelayedSwipeRefreshLayout.java com/mynetdiary/community/common/view/HeightLimiterHelperView.java com/mynetdiary/community/common/view/HeightProbeHelperView.java com/mynetdiary/community/common/view/PrefetchLinearLayoutManager.java com/mynetdiary/community/common/view/a.java com/mynetdiary/community/feed/a.java com/mynetdiary/community/group/data/g.java com/mynetdiary/community/group/data/i.java com/mynetdiary/community/group/data/i.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mynetdiary/community/group/data.java
				com/mynetdiary/community/group/edit/EditGroupViewModel.java
				com/mynetdiary/community/group/edit/a.java
				com/mynetdiary/community/group/membership/MultipleGroupsMembershipViewModel.java
				com/mynetdiary/community/invitation/incoming/SustainedInvitationRepository.java
				com/mynetdiary/community/invitation/outgoing/CreateInvitationViewModel.java
				com/mynetdiary/community/invitation/outgoing/a.java
				com/mynetdiary/community/invitation/outgoing/b.java
				com/mynetdiary/community/invitation/outgoing/e.java
				com/mynetdiary/community/invitation/r.java
				com/mynetdiary/community/invitation/t.java
				com/mynetdiary/community/invitation/y.java
				com/mynetdiary/community/notifications/g0.java
				com/mynetdiary/community/notifications/m.java
				com/mynetdiary/community/notifications/n0.java
				com/mynetdiary/community/post/data/a.java
				com/mynetdiary/community/post/data/c.java
				com/mynetdiary/community/post/edit/EditSuccessStoryViewModel.java
				com/mynetdiary/community/post/edit/c0.java
				com/mynetdiary/community/post/edit/p0.java
				com/mynetdiary/community/profile/AttitudeRepository.java
				com/mynetdiary/community/profile/ProfileRepository.java
				com/mynetdiary/community/profile/ProfileRequestService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				questService.java com/mynetdiary/community/profile/c.java com/mynetdiary/community/profile/connections/UserConnectionsViewModel.java com/mynetdiary/community/profile/connections/a.java com/mynetdiary/community/profile/connections/d.java com/mynetdiary/community/profile/d.java com/mynetdiary/community/profile/e.java com/mynetdiary/community/profile/edit/EditProfileViewModel.java com/mynetdiary/community/profile/edit/a.java com/mynetdiary/community/profile/f.java com/mynetdiary/community/profile/g.java com/mynetdiary/community/profile/h.java com/mynetdiary/community/profile/s0.java com/mynetdiary/community/root/CommunityRootFragment.java com/mynetdiary/community/s.java com/mynetdiary/db/MynetdiaryDatabase.java com/mynetdiary/db/b.java com/mynetdiary/e.java com/mynetdiary/feature/advancedplanning/data/AdvancedAutopilotRemindersWorker.java com/mynetdiary/feature/advancedplanning/presentation/autopilot/activation/o.java com/mynetdiary/feature/advancedplanning/presentation/overview/c.java com/mynetdiary/feature/advancedplanning/presentation/planningtype/PlanningTypeViewModel.java com/mynetdiary/feature/advice/domain/AdviceInteractor.java com/mynetdiary/feature/advice/presentation/b.java com/mynetdiary/feature/fasting/presentation/screens/review/h.java com/mynetdiary/feature/fasting/presentation/widget/config/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/widget/config/a.java com/mynetdiary/feature/integrations/healthc onnect/data/action/u.java
				com/mynetdiary/feature/mealphotos/data/re pository/a.java
				com/mynetdiary/feature/mealphotos/present ation/screens/recognition/MealRecognitionVie wModel.java
				com/mynetdiary/feature/mealphotos/present ation/screens/recognition/k0.java
				com/mynetdiary/feature/streaks/ui/timeline/ TimelineViewModel.java
				com/mynetdiary/implementation/food/f.java
				com/mynetdiary/messaging/fcm/FcmMessagi ngService.java
				com/mynetdiary/messaging/fcm/FcmRegistra tionWorker.java
				com/mynetdiary/messaging/fcm/a.java
				com/mynetdiary/mindersync/MinderSyncThr ead.java
				com/mynetdiary/mindersync/f.java
				com/mynetdiary/multidayanalysis/e.java
				com/mynetdiary/profile/budget/EnergyBudge tViewModel.java
				com/mynetdiary/profile/budget/c.java
				com/mynetdiary/profile/customizing/Customi zingViewModel.java
				com/mynetdiary/profile/customizing/b.java
				com/mynetdiary/profile/dob/DobEditViewMo del.java
				com/mynetdiary/profile/dob/b.java
				com/mynetdiary/profile/height/b.java
				com/mynetdiary/profile/weight/c.java
				com/mynetdiary/profile/weight/e.java
				com/mynetdiary/profile/wizard/WizardViewM odel.java
				com/mynetdiary/profile/wizard/a.java
				com/mynetdiary/profile/wizard/s.java
				com/mynetdiary/profile/wizard/t.java
				com/mynetdiary/subscriptions/MaterialButto nWithCustomBackground.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mynetdiary/subscriptions/UpgradeHighlightHistory.java
				com/mynetdiary/tutorial/view/TouchLimitingConstraintLayout.java
				com/mynetdiary/ui/components/PlayerView.java
				com/mynetdiary/ui/fragments/auth/SplashResyncViewModel.java
				com/mynetdiary/ui/fragments/customfood/CustomFoodFlowFragment.java
				com/mynetdiary/ui/fragments/customfood/b.java
				com/mynetdiary/ui/fragments/mainnav/MainNavigationFragment.java
				com/mynetdiary/ui/fragments/managesubscription/ManageSubscriptionViewModel.java
				com/mynetdiary/ui/fragments/myfoods/n0.java
				com/mynetdiary/ui/fragments/myplan/macronutrients/y.java
				com/mynetdiary/ui/fragments/recipe/o0.java
				com/mynetdiary/ui/fragments/recipe/view/h.java
				com/mynetdiary/ui/fragments/settings/SettingsViewModel.java
				com/mynetdiary/ui/fragments/support/j0.java
				com/mynetdiary/ui/fragments/support/o0.java
				com/mynetdiary/ui/w.java
				com/samsung/android/sdk/healthdata/HealthDataObserver.java
				com/samsung/android/sdk/healthdata/HealthDataStore.java
				com/samsung/android/sdk/healthdata/HealthPermissionManager.java
				com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java
				com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
				com/samsung/android/sdk/internal/healthdat

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthdat a/a.java cv/b.java cv/j.java d0/y0.java de/a.java df/d.java dk/g.java du/d.java dw/a0.java dx/k.java e8/m.java eb0/c.java ed/a.java ed/d.java ed/j.java eh/c.java eu/d.java f30/e.java f5/i.java f5/o.java fb/a.java fg0/i.java fh/b0.java fh/u.java fn0/d.java fv/e.java fv/p.java g00/d0.java g4/c.java g5/d.java gc0/y.java gd/e.java gd/q.java gd/r.java gi/a.java
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	gk/b.java gk/c.java gk/k.java gk/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gl/a.java
				gl/c.java
				gl0/d.java
				gn0/c.java
				gu/g.java
				gx/w.java
				gz/w0.java
				h/e.java
				h20/a.java
				h30/b.java
				h60/m.java
				hd/d.java
				hi/q.java
				hk/d0.java
				hk/e.java
				hk/h.java
				hk/i.java
				hk/i0.java
				hk/l.java
				hk/u.java
				hk/y.java
				hl/a.java
				hl0/b.java
				hl0/g.java
				hm/i.java
				hu/e.java
				hu/f.java
				i2/b.java
				ie0/a.java
				ie0/b.java
				il/e0.java
				il/m.java
				il/n.java
				il/t.java
				il/u.java
				il/u0.java
				il/w.java
				iu/e1.java
				iu/q0.java
				iu/s.java
				iu/w1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ix/b1.java
				iy/a.java
				j5/a0.java
				j5/b.java
				j5/b1.java
				j5/c2.java
				j5/i1.java
				jc/c.java
				jd/d.java
				jd/l.java
				jj/i.java
				jl/c1.java
				jl/d1.java
				jl/e0.java
				jl/f1.java
				jl/q5.java
				jl/r3.java
				jl/r5.java
				jl/s.java
				jl/w5.java
				jl/y5.java
				jl/z5.java
				ju/f0.java
				ju/j1.java
				ju/l1.java
				ju/n.java
				ju/v0.java
				ju/x0.java
				ju/y0.java
				jz/a.java
				k5/t.java
				k7/c.java
				ka/a.java
				ka/n.java
				kb/t.java
				kq/a.java
				kx/f2.java
				kx/h0.java
				kx/y1.java
				kz/a.java
				kz/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				kz/g.java
				kz/j.java
				l60/a.java
				l60/d1.java
				l60/e.java
				l60/f1.java
				l60/h.java
				l60/i.java
				l60/r.java
				l7/a.java
				ld/b.java
				lk/a.java
				ll/h.java
				ln0/f0.java
				lp0/a.java
				lq/b.java
				lq/d.java
				lq/i1.java
				lq/l0.java
				lq/o0.java
				lq/p1.java
				lq/t1.java
				lq/v.java
				lq/z.java
				lq/z0.java
				lu/p.java
				m30/n.java
				m5/c.java
				m60/c.java
				ma/v.java
				mh/a.java
				mh/e.java
				mh/i.java
				mj/a.java
				mp0/c.java
				mp0/d.java
				mq/b.java
				mr/f.java
				mr/l.java
				mr/m.java
				n0/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n60/c.java
				nd/a.java
				nd/a.java
				ng/d.java
				ng/j.java
				nu/q.java
				nu/u.java
				nx/g0.java
				o/c.java
				o4/c.java
				o4/o.java
				oc/a.java
				od/d.java
				oi/p.java
				oj0/a.java
				oq/a.java
				org/conscrypt/Platform.java
				org/conscrypt/ct/CTVerifier.java
				oz/a.java
				p00/b.java
				pc/d.java
				pc/e.java
				pj0/j.java
				pj0/m0.java
				pj0/x.java
				pk/b.java
				pm/e0.java
				pm/g1.java
				pm/i0.java
				pm/n0.java
				pm/n1.java
				pm/o0.java
				pm/t0.java
				pm/u0.java
				pn/a.java
				pn0/a.java
				pq/b.java
				pu/c.java
				qd/a.java
				qi/i.java
				qk/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				qk/r.java
				qk/s.java
				qm/f.java
				qm/n.java
				qn0/d0.java
				qo/o.java
				qo/q.java
				qq/a.java
				qr/a.java
				qr/l.java
				qr/q.java
				qu/d.java
				r0/h.java
				r4/b.java
				r60/g.java
				r60/o.java
				rd/f0.java
				rd/g.java
				rd/p0.java
				rd/z.java
				re0/a.java
				ro0/a.java
				rp/c.java
				ru/f.java
				ru/w.java
				s/d.java
				s/e.java
				s/f.java
				s/h.java
				s/i.java
				s/k.java
				s/l.java
				s00/g.java
				s5/c.java
				s60/m.java
				sa/n.java
				sc/a.java
				sd/c.java
				sd/f.java
				sd/i0.java
				sd/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sh/b.java
				sh/g.java
				so/c.java
				sp/c.java
				t4/a.java
				t4/c.java
				t4/d.java
				t4/f.java
				t7/a.java
				tf0/a0.java
				th/e.java
				ti0/l.java
				ts/c.java
				uc/c.java
				uc/e.java
				uh/c.java
				uk/d.java
				uo/j.java
				up/g.java
				uu/c1.java
				uu/m0.java
				uu/p.java
				uu/y0.java
				uv/a.java
				uv/b.java
				uv/m.java
				uw/i.java
				uw/m.java
				v2/c.java
				v2/g.java
				v50/m.java
				vc/i.java
				vc/j.java
				vd/l.java
				vf0/b.java
				vf0/d.java
				vf0/h.java
				vg/a0.java
				vg/g0.java
				vg/h0.java
				vp/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yp/t.java
				yr/b.java
				vs/f.java
				vs/y.java
				w4/d.java
				w4/e.java
				w4/k.java
				w4/m.java
				w4/z.java
				wc/e.java
				wc/i.java
				wd/c.java
				wd/d.java
				we0/t.java
				wf/d.java
				wh0/c1.java
				wh0/l.java
				wh0/p0.java
				wj/a.java
				wj/d.java
				wj0/u.java
				wj0/v.java
				wl/a.java
				wo/g.java
				wo/h.java
				wo0/c.java
				wo0/e.java
				wo0/g.java
				wo0/h.java
				wq/c.java
				wq/d.java
				wu/a.java
				wu/b.java
				wy/a.java
				xc/a.java
				xf0/b.java
				xf0/f.java
				xf0/g.java
				xn/a0.java
				xn/d0.java
				xn/f.java
				xn/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xn/i.java
				xn/u.java
				xn/y.java
				xq/e.java
				xs0/a.java
				xt/j.java
				xv/b.java
				y4/c.java
				y4/d.java
				y4/h.java
				y50/c.java
				ya/a.java
				yc/c.java
				yc/d.java
				yc/g.java
				yc/t.java
				yc/u.java
				yc/v.java
				yd/a.java
				yj0/j.java
				yl/d.java
				yn/c.java
				yn/f.java
				yp/d.java
				yp/k.java
				yp/n.java
				yt/d0.java
				yt/i.java
				yt/k0.java
				yt/t.java
				yt/w.java
				z/s.java
				z1/t1.java
				z4/f.java
				z4/j.java
				z4/k.java
				z4/m.java
				z4/o.java
				zg/c.java
				zl/b.java
				zt/e.java
				zt/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				~~2~~/1.java ~~zv/y8.java~~
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	ee/b.java fh/a0.java lh/a.java rd/b.java rd/e0.java rd/g0.java rd/i.java rd/p0.java vh/d.java vh/n.java yd/j.java
3	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	a4/i.java a4/t0.java aj/b.java bw/b2.java ca0/e.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/y.java com/mynetdiary/auth/AuthActivity.java com/mynetdiary/professionalsharing/fragment/messages/MessagesViewModel.java com/mynetdiary/ui/fragments/foodentry/c.java dj0/a.java eg0/a.java f8/a.java i2/q1.java i2/w2.java i70/a.java jm0/h2.java ks0/j1.java m00/f0.java n00/a.java n00/d.java n00/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o00/c.java
				n0b.java
				org/conscrypt/OpenSSLECKeyFactory.java
				org/conscrypt/OpenSSLRSAKeyFactory.java
				q60/a.java
				qr/q.java
				sb/d.java
				ss0/d.java
				tc/c.java
				ud/d.java
				up/h.java
				up/m.java
				up/q.java
				up/r.java
				wm/b.java
				yi/g.java
				zz/g.java
				zz/h.java
				zz/i.java
4	[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/mynetdiary/commonsclient/dailyanalysis/presentation/g.java com/mynetdiary/mindersync/e.java com/mynetdiary/ui/fragments/advice/MyAdviceFragment.java il/u.java j8/q1.java ji0/f.java lr0/a.java lr0/b.java mr0/a.java s8/t.java vg/g0.java vh/a.java yo0/c0.java zo0/f.java zo0/g.java zo0/h.java zo0/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	bb/c.java com/mixpanel/android/mpmetrics/MPDbAdapter.java eb0/d.java qj/m0.java qj/v0.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	mr/b.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	eh/a.java pn/a.java ue/b.java ut/b.java y10/d.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/canhub/cropper/CropImageActivity.java d0/a0.java he/a.java od/d.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	he/a.java od/d.java vg/g0.java wq/e.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ae/l.java f80/g.java hc/f.java sd/d.java
12	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	ci/n.java
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	s/i.java
14	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	at/h.java
15	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	hm/v.java

👤 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🖧 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ac/p.java ae/l.java an/e.java be/i.java com/bumptech/glide/load/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java d0/a0.java dr0/g.java dr0/i.java ee/a.java fe/b.java hc/f.java hc/g.java kg/i.java l60/p0.java oc/a.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java ps0/w.java qd/a.java sd/f.java w4/e.java wm/f.java xg/j.java ya/b.java yc/g.java yi/d.java z4/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/u.java com/mynetdiary/apputil/http/h.java com/mynetdiary/ui/fragments/recipe/view/c.java d0/a0.java hc/f.java hc/g.java he/f.java m20/d.java qd/a.java wm/f.java wq/e.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	bi/c.java ci/c1.java com/mynetdiary/community/CommunityQuickActionsService.java com/mynetdiary/feature/fasting/presentation/widget/config/a.java com/mynetdiary/ui/MainActivity.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java f60/b.java fh/b.java gj0/a1.java hk/f.java iq/j.java jl/r5.java ka/a.java ka/n.java vg/a.java vg/a0.java vg/g0.java vg/h0.java vg/l0.java vs/e0.java vs/j0.java yo0/l0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/mynetdiary/auth/AuthActivity.java com/mynetdiary/ui/MainActivity.java com/mynetdiary/ui/WebViewActivity.java fh/e0.java vg/a0.java
00096	Connect to a URL and set request method	command network	com/mixpanel/android/util/a.java g8/i.java hc/b.java rd/z.java sh/b.java ud/d.java uh/d.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java com/mixpanel/android/util/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java eh/c.java g8/i.java sh/b.java ud/d.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java g8/i.java hc/b.java sh/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java com/mixpanel/android/util/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java dk/f.java g8/i.java sh/b.java ud/d.java wj/d.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java g8/i.java zm/a.java
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java g8/i.java
00012	Read data and put it into a buffer stream	file	ae/l.java org/conscrypt/DefaultSSLContextImpl.java sd/f.java
00014	Read file into a stream and put it into a JSON object	file	be/i.java ee/a.java wm/f.java xg/j.java
00005	Get absolute path of file and put it to JSON object	file	wm/f.java
00132	Query The ISO country code	telephony collection	e8/k0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bi/c.java ci/c1.java com/mynetdiary/community/CommunityQuickActionsService.java f60/b.java hk/f.java iq/j.java ka/a.java vg/g0.java vg/h0.java
00036	Get resource file from res/raw directory	reflection	com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/mynetdiary/messaging/fcm/FcmMessagingService.java h60/g.java hk/f.java n20/a.java qd/a.java vg/a.java vg/g0.java vg/h0.java vg/l0.java vs/e0.java vs/j0.java vv/b.java yi/f.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/u.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	d8/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	uc/c.java vg/a0.java
00189	Get the content of a SMS message	sms	qr/b0.java ue/d.java vg/a0.java
00188	Get the address of a SMS message	sms	qr/b0.java ue/d.java vg/a0.java
00200	Query data from the contact list	collection contact	qr/b0.java ue/d.java vg/a0.java
00201	Query data from the call log	collection calllog	qr/b0.java ue/d.java vg/a0.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	k5/t.java
00003	Put the compressed bitmap data into JSON object	camera	rd/z.java vd/l.java
00121	Create a directory	file command	com/mynetdiary/common/images/cropper/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00015	Put buffer stream (data) to JSON object	file	vg/g0.java
00078	Get the network operator name	collection telephony	com/mixpanel/android/mpmetrics/i.java vg/g0.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java vg/g0.java
00191	Get messages in the SMS inbox	sms	vg/a.java vg/a0.java vg/g0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	vg/a0.java
00187	Query a URI and check the result	collection sms calllog calendar	vg/a0.java
00004	Get filename and put it to JSON object	file collection	bh/a.java
00079	Hide the current app's icon	evasion	tb/b0.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/579537168227/namespaces/firebase:fetch?key=AIzaSyD3TKySTaVkNkWd9DPZo7KQJFYJHnZTPeY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'is_trial_prices': 'false', 'show_promo_after_signup': 'false', 'show_trial_after_signup': 'false', 'show_upgrade_on_home_scheduled_2': 'false', 'upgrade_sale_name': ''}, 'state': 'UPDATE', 'templateVersion': '90'}

⁚⁚⁚⁚ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	5/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.ACTIVITY_RECOGNITION, 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
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
assets.mynetdiary.com	ok	**IP:** 18.238.109.123 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
player.vimeo.com	ok	**IP:** 162.159.138.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
www.css	ok	No Geolocation information available.
www.interpretation	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
graph-video.s	ok	No Geolocation information available.
www.mynetdiary.com	ok	**IP:** 100.29.56.54 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
help.fitbit.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.wencodeuricomponent	ok	No Geolocation information available.
mynetdiary.com	ok	**IP:** 76.223.89.109 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
x.giphy.com	ok	**IP:** 199.232.197.155 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 172.253.124.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.world	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.years	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.
www.nccih.nih.gov	ok	**IP:** 18.238.109.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.nal.usda.gov	ok	**IP:** 52.245.234.40 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.251.15.105 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schema.googleapis.com	ok	**IP:** 172.217.215.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.a	ok	No Geolocation information available.
www.hortcut	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.mixpanel.com	ok	**IP:** 35.186.241.51 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 64.233.176.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.manifestations	ok	No Geolocation information available.
www.cdc.gov	ok	**IP:** 23.52.208.211 **Country:** Argentina **Region:** Ciudad Autonoma de Buenos Aires **City:** Buenos Aires **Latitude:** -34.613152 **Longitude:** -58.377232 **View:** Google Map
www.niddk.nih.gov	ok	**IP:** 13.107.246.69 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.33.88.220 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
a2.mynetdiary.com	ok	**IP:** 18.238.96.21 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.in	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pingback.giphy.com	ok	**IP:** 151.101.129.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.language	ok	No Geolocation information available.
api.giphy.com	ok	**IP:** 151.101.193.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.recent	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
hub.samsungapps.com	ok	**IP:** 54.73.22.117 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.139 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
medlineplus.gov	ok	**IP:** 18.238.109.109 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.reddit.com	ok	**IP:** 151.101.129.140 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
fdc.nal.usda.gov	ok	**IP:** 52.245.234.40 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
s3.amazonaws.com	ok	**IP:** 52.216.45.8 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 64.233.185.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.icon	ok	No Geolocation information available.
x-qa.giphy.com	ok	**IP:** 199.232.193.155 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.c	ok	No Geolocation information available.
ods.od.nih.gov	ok	**IP:** 172.65.90.24 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.style	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
.jpg	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
developers.google.com	ok	**IP:** 172.217.215.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.text-decoration	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	hk/t.java
support@mynetdiary.com	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
GIPHY Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/299
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

🔑 HARDCODED SECRETS

POSSIBLE SECRETS

"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"

"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

"com.google.firebase.crashlytics.mapping_file_id" : "c1ddb7150d374ac8b7b3f1e2219e496f"

"community_group_private" : "Private"

"facebook_client_token" : "91252893b3385e851a7cc4f836d879b3"

"google_api_key" : "AIzaSyD3TKySTaVkNkWd9DPZo7KQJFYJHnZTPeY"

"google_crash_reporting_api_key" : "AIzaSyD3TKySTaVkNkWd9DPZo7KQJFYJHnZTPeY"

"password" : "Password"

"turkey" : "Turkey"

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

4447b2b21dd60319442dfb2270e1632ab97288f4

68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166
43812574028291115057151

POSSIBLE SECRETS

308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d010105050500308194310b3009060355040613025553311330110603550408130a436
16c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f6964311030e060355040b1307416e64726f696
43110300e06035504031307416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303232393031333
334365a170d33353037313373031333334365a308194310b30090603550406130255533113301106035504081308130a43616c69666f726e69613116301406035504071307130d4
d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312
2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d003082010802820101008d
6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81b
bfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2cb3f28
4a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e24
7553311c46b9af76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a381fc3081f9301d0603551d0e0416041448
5900563d272c46ae118605a47419ac09ca8c113081c90603551d230481c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b3009
06035504061302555331133011060355040813a43616c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965773110300e060355040a1307416e6
4726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e6
4726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d0101050500003820101007aaf968ceb50c441055118d0daabaf0
15b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824b656dbe4dc22
40912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea5603b2c540dbd
7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430e
ea7c26a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d

---

83f36540ec598155e7294d8ed5284187f82fbf9d

---

d57d566c993ca9c6904e58685a6d1b9b51b2f4ab

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

470fa2b4ae81cd56ecbcda9735803434cec591fa

7f108530ebbe2a35a2132d6247e1196d2e2c3dbb

27408ce1408dac375e4b4a700210ed4a340e84a3

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

af60eb711bd85bc1e4d3e0a462e074eea428a8

bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

d6d3b16b1954b543cd523b9f8affb237

c56fb7d591ba6704df047fd98f535372fea00211

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d

b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4

39402006196394479212279040100143613805079739270465446679469052796276593991132635693989563081522949135544336539 42643

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

36864200e0eaf5284d884a0e77d31646

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

9b8f518b086098de3d77736f9458a3d2f6f95a37

POSSIBLE SECRETS

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

e4c4922badb509858ddfb7825f879b01

b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21

808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f

1a92ae93704243b9ef12c747246832115df22968

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a436
16c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f696
43110300e06035504031307416e64726f696431223020060092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d30383030343135323234
3035305a170d3335303930313232343035305a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307130d4
d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312
2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d0030820108028201010009
c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc
01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37
a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350e
c535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604
144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b30
09060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965773110300e060355040a1307416
e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696431223020060092a864886f70d0109011613616e64726f696440616
e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d010104050003820100572551b8d93a1f73de0f6d469f86d
ad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12
d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc0596
17cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8
399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357

POSSIBLE SECRETS

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

86254750241babac4b8d52996a675549

2e74d42ab02c5a8523f6890dc5e1bca5daaf535a

115792089210356248762697446949407573530086143415290314195533631308867097853951

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

3b25e9acb3273fdd9d9ca48bd125513bf26f4dc1

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

cc2751449a350f668590264ed76692694a80308a

51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124440380340372808892707005449

1cbd3130fa23b59692c061c594c16cc0

63cebbd4932919ab13af3eeac0d201bb9a34a86f

a0784d7a4716f3feb4f64e7f4b39bf04

ab178f552a3baa8cba3f528fad9bb5d8

POSSIBLE SECRETS

308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b5231143012060355040813 0b53
6f757468204b6f72656131133011060355040713a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a0603550
40b1303444d433115301306035504030c53616d73756e672043657274 43125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6
d301e170d313130363232313232323531325a170d33383131303733132323531325a3081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f6f f
726561 31133011060355040713a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43
3115301306035504030c53616d73756e672043657243 43125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d
06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9
b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0de
fcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd1841
1a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec3
5feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b
627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407
130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504030c53
616d73756e6720436572743 43125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d20995a79c0daad6300c0603551d13
040530030101ff300d06092a864886f70d0101050500038201 00329601fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63aace8c019a1a66616
a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299db4bf0b25b
7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512df
b28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9
369c08c810158

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS

308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b3009060355040613024b523114301206035504081305356f757468204b6f72656131133011060355040713ca5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031305306c53616d73756e67204365727443125302306092a864886f70d0109011616616e64726f69642e6f73406d73756e672e636f6d301e170d3131303632323231323235313335a170d33383131303073132323531335a3081a2310b3009060355040613024b523114301206035504081305356f757468204b6f72656131133011060355040713ca5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031305306c53616d73756e67204365727443125302306092a864886f70d0109011616616e64726f69642e6f73406d73756e672e636f6d30820120300d006092a864886f70d0101010500038201d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b3009060355040613024b523114301206035504081305356f757468204b6f72656131133011060355040713ca5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031305306c53616d73756e67204365727443125302306092a864886f70d0109011616616e64726f69642e6f73406d73756e672e636f6d820900e5eff0a8f66d92b3300c06035551d13040530030101ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

bae8e37fc83441b16034566b

308201e53082014ea00302010202044f54468b300d06092a864886f70d01010505003037310b3009060355040613025533110300e060355040a1307416e64726f69643116301406035504031305416e64726f69642044656275673019f300d06092a864886f70d010101050003818d0030818902818100a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c5990503279827346bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf918702030100011300d06092a864886f70d0101050500038181000512992268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122

5cfc94a12baeaa5a62f5f3585c304ef3c06574dd

POSSIBLE SECRETS
11579208921035624876269744694940757352999695522413576034242225906106851204436

▶ PLAYSTORE INFORMATION

Title: Calorie Counter - MyNetDiary

Score: 4.701957 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support: Category:** Health & Fitness **Play Store URL:** com.fourtechnologies.mynetdiary.ad

Developer Details: MyNetDiary.com, MyNetDiary.com, None, https://www.mynetdiary.com, support@mynetdiary.com,

Release Date: Sep 17, 2010 **Privacy Policy:** Privacy link

Description:

Track calories, food, and macros with ease! MyNetDiary has a free barcode scanner, personal diet plans, and AI Meal Scan for instant logging — all in a smart, simple-to-use app. Ranked #1 in Forbes Health's Best Weight Loss Apps of 2025. Rated #1 by the American Journal of Preventive Medicine. The best all-around healthy lifestyle app. The New York Times calls it "simpler, quicker, nicer" compared to similar apps. Selected by Today's Dietitian Magazine for its Popular Weight Loss Apps list alongside WW and Noom. Dietitians and personal trainers choose MyNetDiary Professional Connect to work with their clients. Unlike other diet apps, MyNetDiary is easy to navigate, includes generous free features, and has no ads. The free calorie counter is totally sufficient for successful weight loss. MyNetDiary forces nothing on you. You can choose one of the popular diets, follow the tips prepared by our Registered Dietitians, consider personalized advice offered by Virtual Coach, or simply enjoy the best calorie counter app on your smartphone and smartwatch. MyNetDiary has the largest verified food database - over 1.7 million items and 107 nutrients, making it the most reliable food tracker ever! Your food diary will show the most accurate nutrition, for all macros, vitamins, minerals, omega fats - all nutrients considered. PROVEN SUCCESS • Active members achieve average weight loss of 1.4 lb each week • Over 25 million members, a great number of experienced dieters switch from other apps Free Calorie Tracker features include: • Lightning-fast food journal with barcode scanner, instant search, and AI-powered Voice Food Log taking only seconds to enter your foods • Robust mega-database of food labels verified and updated daily with restaurants, grocery stores, special diets, and ethnic foods • Exercise tracker supporting over 500 types of exercise and recreation • Daily coaching advice • Customizable dashboard: you control how the app looks and works • Wear OS app with tiles & complications: log foods and amount by saying what you ate, track consumed water and body weight. Keep an eye on daily carbs / fat / protein breakdown and a quick daily summary. • Health Connect, Google Fit and Samsung Health integration • Custom Food Editor and Recipe Editor • Water Tracker • Steps Tracker • Configurable Reminders • Shopping list for foods and any other grocery items • Motivating diet and nutrition articles written by our Registered Dietitians • Professional Connect: free and easy - connect with your dietitian or trainer via MyNetDiary to share your data and use their professional guidance • Community of people supporting each other in their weight loss journey • Total data privacy and protection - no account required MyNetDiary Premium provides all the guidance and features you may need for the best results: • Premium Diets, including Low-Carb, Keto, High-Protein, Mediterranean, Vegetarian, Vegan and more - with a diet plan, guides and feedback. • Intermittent fasting tracker: popular and custom protocols, special timer and reports • Autopilot adjusts your calorie budget automatically, guiding you to your goal weight • Up to 50 Health Trackers: blood pressure, cholesterol, blood glucose, A1C, ketones, medications, symptoms, and body measurements • 600 Premium Recipes and 200 Premium Meals developed by our Registered Dietitians - delicious, easy to cook and customize • Premium Menus (Meal Plans) help you plan and balance your nutrition throughout the week • Recipe Import loads your favorite recipes from the web and calculates complete nutrition automatically • Recipe Database with over 370,000 dishes and

detailed nutrition facts • Integrations with Fitbit, Garmin, and Withings • Track up to 107 nutrients, set custom targets, get the recommendations for optimal nutrition.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:31:12	Generating Hashes	OK
2025-08-29 22:31:22	Extracting APK	OK
2025-08-29 22:31:22	Unzipping	OK
2025-08-29 22:31:54	Parsing APK with androguard	OK
2025-08-29 22:31:54	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:31:55	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:32:00	Parsing AndroidManifest.xml	OK
2025-08-29 22:32:00	Extracting Manifest Data	OK

2025-08-29 22:32:00	Manifest Analysis Started	OK
2025-08-29 22:32:00	Performing Static Analysis on: MyNetDiary (com.fourtechnologies.mynetdiary.ad)	OK
2025-08-29 22:32:01	Fetching Details from Play Store: com.fourtechnologies.mynetdiary.ad	OK
2025-08-29 22:32:01	Checking for Malware Permissions	OK
2025-08-29 22:32:01	Fetching icon path	OK
2025-08-29 22:32:01	Library Binary Analysis Started	OK
2025-08-29 22:32:01	Reading Code Signing Certificate	OK
2025-08-29 22:32:02	Running APKiD 2.1.5	OK
2025-08-29 22:32:12	Detecting Trackers	OK
2025-08-29 22:32:18	Decompiling APK to Java with JADX	OK
2025-08-29 22:32:52	Converting DEX to Smali	OK

2025-08-29 22:32:52	Code Analysis Started on - java_source	OK
2025-08-29 22:33:01	Android SBOM Analysis Completed	OK
2025-08-29 22:33:16	Android SAST Completed	OK
2025-08-29 22:33:16	Android API Analysis Started	OK
2025-08-29 22:33:29	Android API Analysis Completed	OK
2025-08-29 22:33:30	Android Permission Mapping Started	OK
2025-08-29 22:33:54	Android Permission Mapping Completed	OK
2025-08-29 22:34:07	Android Behaviour Analysis Started	OK
2025-08-29 22:34:28	Android Behaviour Analysis Completed	OK
2025-08-29 22:34:28	Extracting Emails and URLs from Source Code	OK

2025-08-29 22:34:40	Email and URL Extraction Completed	OK
2025-08-29 22:34:41	Extracting String data from APK	OK
2025-08-29 22:34:41	Extracting String data from Code	OK
2025-08-29 22:34:41	Extracting String values and entropies from Code	OK
2025-08-29 22:34:53	Performing Malware check on extracted domains	OK
2025-08-29 22:35:02	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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