MOBSF

ANDROID STATIC ANALYSIS REPORT

Trendsales (4.7.2)

File Name:	Trendsales _ Fashion & Home_4.7.2_Apkpure.apk
Package Name:	com.tradono.android
Scan Date:	May 25, 2023, 8:43 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	15	1	1	2

FILE INFORMATION

File Name: Trendsales _ Fashion & Home_4.7.2_Apkpure.apk
Size: 79.26MB
MD5: 8ed543e46858f2f4ccd9c338e4bf67a8
SHA1: f368505d31d9d1b10e8bf347b01534ad448683e1
SHA256: ce9c75da5c1c788811e485ae50f77af83c903b53bbea17544b4334949fd10eef

APP INFORMATION

App Name: Trendsales
Package Name: com.tradono.android
Main Activity: com.tradono.android.ui.login.root.RootActivity
Target SDK: 32
Min SDK: 21
Max SDK:
Android Version Name: 4.7.2

Android Version Code: 891

APP COMPONENTS

Activities: 140
Services: 16
Receivers: 20
Providers: 8
Exported Activities: 4
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: OU=Tradono
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-02-11 13:10:02+00:00
Valid To: 2040-02-05 13:10:02+00:00
Issuer: OU=Tradono
Serial Number: 0x65ce4f06
Hash Algorithm: sha256
md5: b7b4d63cad2c26d621a44c07489a7f1a
sha1: bf055ff1fe9258d31b643ab83073a94d22af2a77
sha256: faee4afb633d3a968ba3654a9d57471cbbd8056357bdf4c1c8ee8a583b42ceac
sha512: 4f3a087e0b71d93175b114e88a44a0900d2c1624e1a9dd1856764af704bb10eb277627c9c0b5651323dc657a8c30e5bc7d8fb91719d4aa4068b8a985a03eb4bd
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b228c21c4e1daf8af9baefa4a06d73b6a68dd2243590dfd8dab973e818a72aa9

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.tradono.android.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
com.tradono.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
assets/audience_network.dex	FINDINGS: DETAILS Anti Debug Code: Debug.isDebuggerConnected() check Anti-VM Code: possible Build.SERIAL check Compiler: unknown (please file detection issue!)

FILE	DETAILS
classes.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.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Obfuscator</td><td>DexGuard</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
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>
</td></tr>
<tr><td>classes3.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
com.tradono.android.login.magic.MagicLinkDeepLinkActivity	Schemes: https://, trendsales://, Hosts: magic-link.trendsales.com, trendsales.dk, trendsales.com, auth, Paths: /auth,

ACTIVITY	INTENT
com.tradono.android.ui.login.root.RootActivity	Schemes: tradono://, trendsales://, http://, https://, Hosts: tradono.com, tradono.dk, trendsales.com, trendsales.dk, www.tradono.com, www.tradono.dk, www.trendsales.com, www.trendsales.dk, trendsales.page.link,
com.stripe.android.payments.StripeBrowserLauncherActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.tradono.android,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.tradono.android,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	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
5	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.
6	Broadcast Receiver (com.clevertap.android.pushsdk.unregisterForContextMenu) 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: **1** | WARNING: **8** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/danikula/videocache/StorageUtils.java com/tradono/android/component/camera/GalleryButton.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	coil/request/ImageResult.java coil/request/Parameters.java coil/util/ImageLoaderOptions.java com/clevertap/android/sdk/Constants.java com/leanplum/internal/ApiConfigLoader.java com/leanplum/internal/Constants.java com/stripe/android/EphemeralKey.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/parsers/EphemeralKeyJsonParser.java com/stripe/android/paymentsheet/PaymentSheet.java com/stripe/android/paymentsheet/flowcontroller/InitData.java com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/utils/ParcelUtils.java com/stripe/android/view/PaymentAuthWebViewClient.java com/tradono/android/model/entities/auth/EmailLoginRequest.java com/tradono/android/model/requests/UserInfoRequest.java com/tradono/android/model/responses/PaymentIntentConfirmResponse.java
				com/canhub/cropper/CropOverlayView.java com/canhub/cropper/utils/GetUriForFileKt.java com/clevertap/android/pushtemplates/PTLog.java com/clevertap/android/sdk/Logger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/clevertap/android/sdk/displayunits/CTDisplayUnitType.java com/clevertap/android/sdk/response/CleverTapResponse.java com/leanplum/ActionArgs.java com/leanplum/ActionContext.java com/leanplum/FirebaseUtilKt.java com/leanplum/LeanplumCloudMessagingProvider.java com/leanplum/LeanplumFcmProvider.java com/leanplum/LeanplumJobStartReceiver.java com/leanplum/Var.java com/leanplum/internal/AESCrypt.java com/leanplum/internal/ApiConfigLoader.java com/leanplum/internal/JsonConverter.java com/leanplum/internal/LeanplumEventDataManager.java com/leanplum/internal/Log.java com/leanplum/internal/RequestBuilder.java com/leanplum/internal/ResourceQualifiers.java com/leanplum/internal/WebSocketClient.java com/leanplum/internal/http/NetworkOperation.java com/leanplum/internal/http/UploadOperation.java com/leanplum/messagetemplates/options/BaseMessageOptions.java com/leanplum/migration/ResponseHandler.java com/leanplum/monitoring/ExceptionHandler.java com/leanplum/utils/BitmapUtil.java com/stripe/android/Logger.java com/stripe/android/stripe3ds2/transaction/Logger.java com/tradono/android/login/magic/MagicLinkDeepLinkActivity.java com/tradono/android/login/onboarding/OnBoardingLoggedInActivity.java com/tradono/android/utils/extensions/Backgro

NO	ISSUE	SEVERITY	STANDARDS	FILES
				undTasksExtensionsKt$registerPersistentCacheWorker$1$1.java net/danlew/android/joda/TimeZoneChangedReceiver.java org/slf4j/helpers/Util.java org/slf4j/impl/AndroidLoggerAdapter.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/clevertap/android/sdk/network/SSLContextBuilder.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/clevertap/android/pushsdk/setContentView.java j$/util/concurrent/ThreadLocalRandom.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/leanplum/internal/AESCrypt.java
7	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	com/danikula/videocache/ProxyCacheUtils.java com/leanplum/internal/AESCrypt.java
8	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/danikula/videocache/sourcestorage/DatabaseSourceInfoStorage.java com/leanplum/internal/LeanplumEventDataManager.java
9	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/clevertap/android/sdk/inapp/CTInAppBaseFullHtmlFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/nimbusds/jose/crypto/impl/RSA_OAEP.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/clevertap/android/sdk/BuildConfig.java com/nimbusds/jose/jwk/Curve.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libcrashlytics-common.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libcrashlytics-trampoline.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	False warning Symbols are available.
3	lib/armeabi-v7a/libface_detector_v2_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/armeabi-v7a/libcrashlytics.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.
5	lib/armeabi-v7a/libcrashlytics-handler.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/x86/libcrashlytics-common.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
7	lib/x86/libcrashlytics-trampoline.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/x86/libface_detector_v2_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
9	lib/x86/libcrashlytics.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/x86/libcrashlytics-handler.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.
11	lib/arm64-v8a/libcrashlytics-common.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/arm64-v8a/libcrashlytics-trampoline.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	False warning Symbols are available.
13	lib/arm64-v8a/libface_detector_v2_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/arm64-v8a/libcrashlytics.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.
15	lib/arm64-v8a/libcrashlytics-handler.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/x86_64/libcrashlytics-common.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
17	lib/x86_64/libcrashlytics-trampoline.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/x86_64/libface_detector_v2_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	True info Symbols are stripped.
19	lib/x86_64/libcrashlytics.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/x86_64/libcrashlytics-handler.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
static.wizrocket.com	ok	**IP:** 52.85.49.33 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
tradono.zendesk.com	ok	**IP:** 162.159.128.7 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
tradono.dk	ok	**IP:** 63.35.208.234 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tradono-android.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.dao.as	ok	**IP:** 52.174.193.210 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api-dev-2.tradono.com	ok	**IP:** 54.77.207.12 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tracking.bring.com	ok	**IP:** 51.107.209.39 **Country:** Norway **Region:** Oslo **City:** Oslo **Latitude:** 59.912731 **Longitude:** 10.746090 **View:** Google Map
api.dataforsyningen.dk	ok	**IP:** 188.64.158.195 **Country:** Denmark **Region:** Hovedstaden **City:** Frederiksberg **Latitude:** 55.679379 **Longitude:** 12.534630 **View:** Google Map
api-dev.tradono.com	ok	**IP:** 52.48.163.39 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.tensorflow.org	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
velkommen.trendsales.dk	ok	**IP:** 198.49.23.145 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map
trendsales.com	ok	**IP:** 63.35.208.234 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
hooks.stripe.com	ok	**IP:** 54.170.183.1 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
system.etrack1.com	ok	**IP:** 213.174.77.231 **Country:** Denmark **Region:** Midtjylland **City:** Tranbjerg **Latitude:** 56.090099 **Longitude:** 10.119370 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crashpad.chromium.org	ok	**IP:** 142.250.74.115 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.tradono.com	ok	**IP:** 52.208.176.243 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
blog.tradono.dk	ok	**IP:** 198.185.159.145 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map
blog.trendsales.dk	ok	**IP:** 198.49.23.144 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
help.trendsales.dk	ok	**IP:** 34.224.144.42 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
trendsales.dk	ok	**IP:** 63.35.208.234 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.slf4j.org	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
climate.stripe.com	ok	**IP:** 52.49.17.168 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.stripe.com	ok	**IP:** 44.237.95.147 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
about.trendsales.dk	ok	**IP:** 198.185.159.144 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
support@trendsales.dk feedback@trendsales.dk peter@petersen.dk	Android String Resource
android-sdk-releaser@vovr17.prod	lib/armeabi-v7a/libface_detector_v2_jni.so
android-sdk-releaser@vovr17.prod	lib/x86/libface_detector_v2_jni.so
android-sdk-releaser@vovr17.prod	lib/arm64-v8a/libface_detector_v2_jni.so
android-sdk-releaser@vovr17.prod	lib/x86_64/libface_detector_v2_jni.so

TRACKERS

TRACKER	CATEGORIES	URL
CleverTap	Analytics, Profiling, Location	https://reports.exodus-privacy.eu.org/trackers/174
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
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
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
LeanPlum	Analytics, Profiling, Location	https://reports.exodus-privacy.eu.org/trackers/28

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "570a108d4a3071aa976ce0150b61b3d2"
"firebase_database_url" : "https://tradono-android.firebaseio.com"
"google_api_key" : "AIzaSyBzY8x_mOJYl3mD7kVl3Rr224uIGuS56Bs"
"google_crash_reporting_api_key" : "AIzaSyBzY8x_mOJYl3mD7kVl3Rr224uIGuS56Bs"
"stripe_prod_key" : "pk_live_9eBG7goxEKPIOfwIlnbtI5Ja"
"stripe_test_key" : "pk_test_A8fDooWVdQZwtQAJTOuDbHAR"
"url_block_user" : "https://help.trendsales.dk/da/articles/69-blokering-af-beskeder-fra-en-bruger"
"user_authentification_installments_continue_button" : "Continue"
"write_private_small_case" : "Contact"
"url_block_user" : "https://help.trendsales.dk/da/articles/69-blokering-af-beskeder-fra-en-bruger"

POSSIBLE SECRETS
"user_authentification_installments_continue_button" : "Fortsæt"
"write_private_small_case" : "Kontakt"

PLAYSTORE INFORMATION

Title: Trendsales | Fashion & Home

Score: 0 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Shopping **Play Store URL:** com.tradono.android

Developer Details: Trendsales A/S, 8692255980993309790, Vestergade 18B, 1. 1456 København K, https://trendsales.dk, support@trendsales.dk,

Release Date: None **Privacy Policy:** Privacy link

Description:

Denmark’s biggest marketplace for secondhand fashion & lifestyle. Trendsales makes it easy, fast and secure to buy secondhand online. You will get access to Denmark’s biggest selection of secondhand fashion & lifestyle: +1 million users are ready to make a good deal with more than +250.000 new items every month. SAFE TRADES: When you trade via Trendsales, you are insured for up to 100.000 DKK, so you can buy and sell safely. If an item is not as described or it is lost or damaged in shipping you are guaranteed to get your money back. EASY AND CHEAP SHIPPING: When you trade via Trendsales, you’ll get Denmark's cheapest, insured and trackable shipping. We work together with DAO to offer you a secure and fast service, plus a discount on shipping. BUY NOW! PAY LATER: Did you find the perfect item, but don’t have the money now? No problem! When you trade via Trendsales, you can choose to buy now and pay in 10, 20 or 30 days. PAY WITH MOBILEPAY: Easy and fast payment with MobilePay. When you pay with MobilePay within the Trendsales app, you are automatically insured. It has never been easier or safer to trade secondhand online. BOOST YOUR ITEMS: Trendsales offers you great opportunities for a fast sale by boosting your items or your shop. By boosting your items and shop, you will get exposed to more users which increases your chances of selling your items faster. Trendsales gives you the opportunity to find exactly what you were looking for – or find what you didn’t know you were looking for. Download the Trendsales app today and get started selling and buying secondhand fashion & lifestyle online. Trendsales merged with Tradono on May 5th 2019. Users from the old Tradono and Trendsales are now all gathered on the Trendsales app.
