APP SCORES

Security Score **48/100**

Trackers Detection **5/432**

FILE INFORMATION

File Name com.handelsbanken.mobile.android_11.1.2-11112_minAPI24_arm64-v8a_armeabi-v7a_nodpi_apkmirror.com.apk

Size 61.17MB

MD5 04ecdc7ff22bcb2f72224111e4b1c051

SHA1 fdc41070e1444500305dee8ea1bf5cd358565506

SHA256 1282dba2799e7e46d5a2364c73fa9c55e409d78ff7b22ed1df64fcc56a95b4c6

APP INFORMATION

App Name Handelsbanken

Package Name com.handelsbanken.mobile.android

Main Activity com.handelsbanken.mobile.android.SePrivOpenStart

Target SDK 29 Min SDK 24 Max SDK

Android Version Name 11.1.2 Android Version Code 11112

PLAYSTORE INFORMATION

Title Handelsbanken SE – Privat

Score 3.1052632 Installs 1,000,000+ Price 0 Android Version Support Category Finance Play Store URL com.handelsbanken.mobile.android

Developer Svenska Handelsbanken AB (publ), Developer ID Svenska+Handelsbanken+AB+(publ)

Developer Address None

Developer Website http://www.handelsbanken.se/

Developer Email mobil@handelsbanken.se

Release Date Jun 21, 2010 Privacy Policy Privacy link

Description

Det är viktigt för oss att de tjänster du använder mest ska vara enkla och snabba. På startsidan kan du till exempel välja vilka konton, kort eller genvägar du vill se. Du kan också sortera i menyn och har alla inställningar samlade på ett ställe. Med appen har du alltid koll på din ekonomi.

I appen kan du bland annat:

- Hantera dina konton och kort
- Göra betalningar, överföringar och godkänna e-fakturor
- Skanna dina räkningar
- Starta fondsparande, innehav i depå och Investeringssparkonto
- Ta del av Handelsbankens aktieanalyser, experters marknadssyn och dagliga marknadskommentarer
- Se pensionssparande
- Se låneinformation, villkorsändra bolån och se dagens boräntor
- Ansök om lån eller lånelöfte och göra lånekalkyl
- Få koll på din ekonomi med funktionen Min ekonomi
- Beställa Mobilt BankID till en ny enhet

För att logga in behöver du ett avtal om telefontjänster. Avtalet tecknar du via internetbanken under menyvalet Mobil och BankID. Du loggar in med en personlig kod eller med Mobilt BankID.

Behöver du hjälp? Välkommen att kontakta oss dygnet runt på Personlig service 0771-77 88 99.

3 / 180

EXPORTED ACTIVITIES

View All

0 / 13

EXPORTED SERVICES

View All

1 / 4

EXPORTED RECEIVERS

View All

1 / 5

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=SE, ST=Sverige, L=MOBI, O=Svenska Handelsbanken AB (publ), OU=MOBI, CN=Handelsbanken-MOBI
Signature Algorithm: dsa
Valid From: 2010-06-11 09:54:18+00:00
Valid To: 2037-10-27 09:54:18+00:00
Issuer: C=SE, ST=Sverige, L=MOBI, O=Svenska Handelsbanken AB (publ), OU=MOBI, CN=Handelsbanken-MOBI
Serial Number: 0x4c1207ca
Hash Algorithm: sha1
md5: 4121c077c6233cfbbb6b31e678ab82f2
sha1: 7ea5ec8e752e0ae79c45c7741325e061635c2f69
sha256: a668d1c05a5e892e87ed6b0edd5815a8d5b28306efe005f840a3a1b1ece99f55
sha512: b1bab0b191292411014f0238d6434b9385e549df4308ce6f29d069b5871764d5aa648689b109d54f0849e9ccf3dd73ed402d557647b4688dd385ef4d7bf1de8d
PublicKey Algorithm: dsa
Bit Size: 1024
Fingerprint: 4aeef747fd881355bb704c94c75108c8c4d9e5155e7995f034827cf3b2c8fb1e
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.	
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.	
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.	
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.	
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.	

Showing 1 to 10 of 10 entries

Previous 1 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	

API	FILES
Execute OS Command	
Get Installed Applications	
Get Network Interface information	

Showing 1 to 10 of 32 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.google.android.gms.tagmanager.TagManagerPreviewActivity	**Schemes**: tagmanager.c.com.handelsbanken.mobile.android://,

Showing 1 to 1 of 1 entries

Previous 1 Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
1	0	1

Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	5	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	**Content Provider** (com.handelsbanken.android.resources.utils.PdfProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
3	**Activity** (com.handelsbanken.android.resources.office.OfficeListActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.	
4	**Activity** (com.handelsbanken.android.resources.push.landingpage.NotificationInformationActivity) 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.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
6	**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.	

Showing 1 to 6 of 6 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
2	7	1	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	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		
2	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		
3	The App uses an insecure Random Number Generator.	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6		
4	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/handelsbanken/android/resources/InetActivity.java	
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4	j/f0/c.java org/acra/f/a.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
6	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		
7	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2	e/e/a/a0/a.java f/a/a/a.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		
9	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	f/a/a/a.java	
10	The file or SharedPreference is World Writable. Any App can write to the file	high	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	e/b/a/b/h/j/b3.java	

Showing 1 to 10 of 12 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

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

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

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

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

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

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

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

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

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

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

Showing 1 to 10 of 20 entries

Previous 1 2 Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://se-priv-mobilapp.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/911676221273/namespaces/firebase:fetch?key=AIzaSyAcleLcRgJbYxyT4A6dmdBDdC3eAfSwFJ0. This is indicated by the response: {'state': 'NO_TEMPLATE'}

Showing 1 to 2 of 2 entries

Previous 1 Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check network operator name check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.MANUFACTURER check
Compiler	r8 without marker (suspicious)

Showing 1 to 3 of 3 entries

Previous 1 Next

lib/arm64-v8a/libTfaAndroid.so

Search:

FINDINGS	DETAILS
Obfuscator	Arxan

Showing 1 to 1 of 1 entries

Previous 1 Next

DEX	DETECTIONS
lib/armeabi-v7a/libTfaAndroid.so	Search: FINDINGS: Obfuscator — DETAILS: Arxan Showing 1 to 1 of 1 entries Previous 1 Next

Showing 1 to 4 of 4 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	com/handelsbanken/android/resources/development/IssueReportActivity.java
00011	Query data from URI (SMS, CALLLOGS)	sms, calllog, collection	e/b/a/b/h/c/b6.java e/b/a/b/h/j/b2.java
00012	Read data and put it into a buffer stream	file	c/j/a/a.java org/acra/g/c.java
00013	Read file and put it into a stream	file	

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil/util/m.java f/a/a/a.java org/acra/g/d.java
00024	Write file after Base64 decoding	reflection file	org/acra/k/e.java
00028	Read file from assets directory	file	com/handelsbanken/android/ocr/q/e.java
00030	Connect to the remote server through the given URL	network	
00036	Get resource file from res/raw directory	reflection	
00039	Start a web server	control network	f/a/a/a.java

Showing 1 to 10 of 27 entries

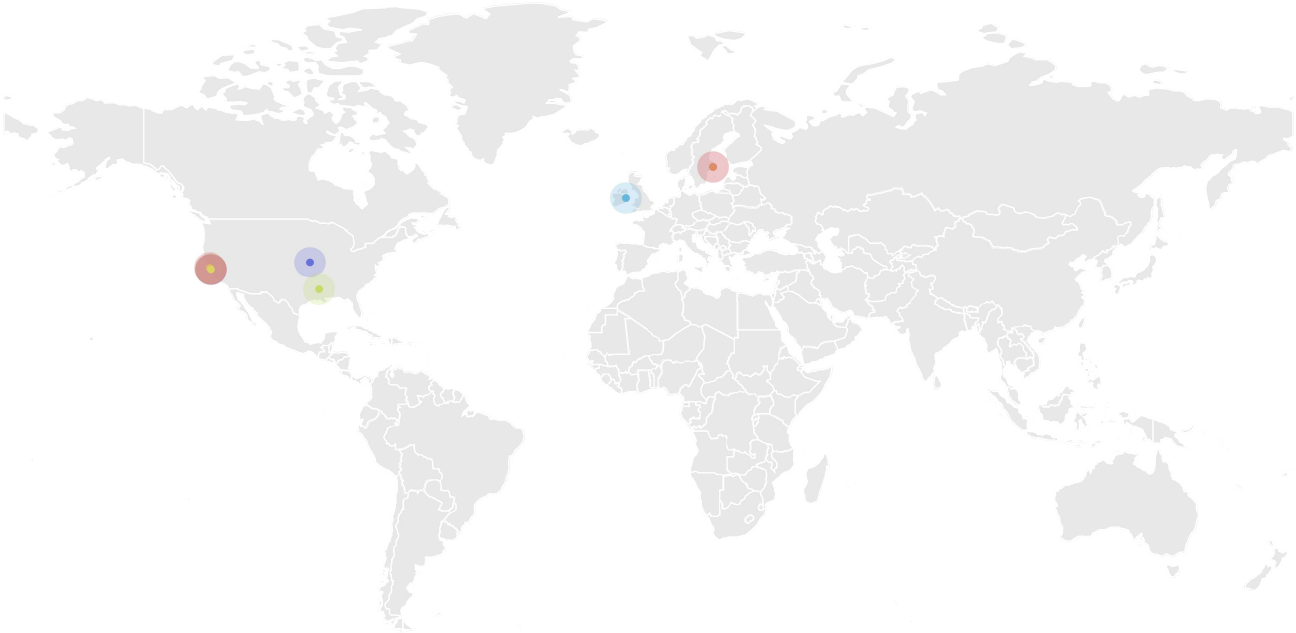
Previous 1 2 3 Next

ABUSED PERMISSIONS

Top Malware Permissions	8/25	Other Common Permissions	2/44
android.permission.READ_CONTACTS, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK		com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	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
docs.google.com	ok	**IP:** 142.250.74.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 4.225.11.194 **Country:** United States of America **Region:** Louisiana **City:** Monroe **Latitude:** 32.548328 **Longitude:** -92.045235 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.handelsbanken.se	ok	**IP:** 192.176.124.165 **Country:** Sweden **Region:** Stockholms lan **City:** Taby **Latitude:** 59.443901 **Longitude:** 18.068720 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	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
schemas.android.com	ok	No Geolocation information available.
se-priv-mobilapp.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

Showing 1 to 10 of 17 entries

Previous 1 2 Next

URLS

Search:

URL	FILE
data::class.java)	com/handelsbanken/android/resources/k.java
data::class.java)	com/handelsbanken/android/resources/bottomnavigation/f.java
http://goo.gl/8rd3yj	e/b/a/b/h/h/n1.java
http://goo.gl/8rd3yj	e/b/a/b/h/h/z.java
http://goo.gl/nafqqk	e/b/a/b/h/h/e.java
http://hostname/?	e/b/a/b/h/h/o3.java

URL	FILE
http://localhost:4949?token=	com/handelsbanken/mobile/android/einvoice/EInvoicesArchiveActivity.java
http://localhost:4949?token=	com/handelsbanken/mobile/android/einvoice/o1.java
http://localhost:4949?token=	com/handelsbanken/mobile/android/payment/m0.java
http://localhost:4949?token=	com/handelsbanken/mobile/android/payment/n0.java

Showing 1 to 10 of 27 entries

Previous 1 2 3 Next

EMAILS

Search:

EMAIL	FILE
this@fundadapter.context	com/handelsbanken/mobile/swedeninvest/market/a/a.java
this@sgpicker2view.picker_pla this@sgpicker2view.picker_top	se/handelsbanken/android/styleguide/lib/view/t.java
u0013android@android.com u0013android@android.com0	e/b/a/b/e/c0.java

Showing 1 to 3 of 3 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
ACRA	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/444
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

Showing 1 to 5 of 5 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **63** secrets

"securekey_session_personal_id" : "secure-session-personal-id"
"firebase_database_url" : "https://se-priv-mobilapp.firebaseio.com"
"docker_header_key" : "X-SHB-APP-TEST-CONTAINER"
"activation_password" : "Salasana"
"activation_enter_user_name" : "Användarkod"
"rel_key_exchange" : "key-exchange"
"numpad_key_prev" : "Tidigare"
"numpad_key_done" : "Valmis"
"rel_push_token" : "push-token"
"numpad_key_done" : "Done"
"activation_enter_user_name" : "Käyttäjätunnus"
"numpad_key_prev" : "Previous"
"numpad_key_done" : "Klar"
"rel_authenticate" : "authenticate"

"button_authorise" : "Godkänn"
"numpad_key_next" : "Next"
"calculate_private_loan_title" : "Privatlån"
"securekey_personal_id" : "secure-personal-id"
"mobi_server_api_version" : "3.6:11.3"
"google_api_key" : "AIzaSyAcleLcRgJbYxyT4A6dmdBDdC3eAfSwFJ0"
"activation_enter_user_name" : "Username"
"menu_mobi_secure_api_version" : "Secure"
"numpad_key_next" : "Seuraava"
"numpad_key_next" : "Nästa"
"rel_codeapp_authenticate" : "authenticate"
"numpad_key_prev" : "Edeltävä"
"menu_mobi_open_api_version" : "Open"
"activation_password" : "Lösenord"
"button_authorise" : "Authorise"
"activation_password" : "Password"
"card_offer_private_const" : "PRIVATE"
"push_debug_input_body_key" : "Body"
"rel_inet_private_loan_information" : "infopage-loan-private"
"rel_htpp_authorizations" : "authorizations"
"rel_authorize_mandate" : "authorizeMandate"
"rel_authorize" : "authorize"
"google_crash_reporting_api_key" : "AIzaSyAcleLcRgJbYxyT4A6dmdBDdC3eAfSwFJ0"
"numpad_key_next" : "Naast"
"numpad_key_prev" : "Vorig"
"numpad_key_done" : "Gereed"
36134250956749795798585127919587881956611106672985015071877198253568414405109
55066263022277343669578718895168534326250603453777594175500187360389116729240
11579208923731619542357098500868790785283756427907490438260516314151816149433 7
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
41058363725152142129326129780047268409114441015993725554835256314039467401291
470fa2b4ae81cd56ecbcda9735803434cec591fa
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965808101243442775783767 84

115792089210356248762697446949407573530086143415290314195533631308867097853948
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123196864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715115792089210356248762697446949407573529996955224135760342422259061068512044369
115792089237316195423570985008687907853269984665640564039457584007908834671663
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598484
115792089210356248762697446949407573530086143415290314195533631308867097853951
484395612939064517590525852527979142027629495260417479958440807170824046352866864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984646
275801935599597058778490118403890480930569058563615685214287073019886892413098608651362607648837451077654397612305753267051002075881697808308513050704318447127338065924327593890433575757337482424

A STRINGS

From APK Resource

▶ Show all **11992** strings

From Code

▶ Show all **27183** strings

From Shared Objects

apktool_out/lib/arm64-v8a/libjpgt.so

▶ Show all **130** strings

apktool_out/lib/arm64-v8a/liblept.so

▶ Show all **5780** strings

apktool_out/lib/arm64-v8a/libpngt.so

▶ Show all **297** strings

apktool_out/lib/arm64-v8a/libtess.so

▶ Show all **2856** strings

apktool_out/lib/arm64-v8a/libTfaAndroid.so

▶ Show all **496** strings

apktool_out/lib/armeabi-v7a/libjpgt.so

▶ Show all **127** strings

apktool_out/lib/armeabi-v7a/liblept.so

▶ Show all **4164** strings

apktool_out/lib/armeabi-v7a/libpngt.so

▶ Show all **69** strings

apktool_out/lib/armeabi-v7a/libtess.so

▶ Show all **1937** strings

apktool_out/lib/armeabi-v7a/libTfaAndroid.so

▶ Show all **542** strings

lib/arm64-v8a/libjpgt.so

▶ Show all **130** strings

lib/arm64-v8a/liblept.so

▶ Show all **5780** strings

lib/arm64-v8a/libpngt.so

▶ Show all **297** strings

lib/arm64-v8a/libtess.so

▶ Show all **2856** strings

lib/arm64-v8a/libTfaAndroid.so

▶ Show all **496** strings

lib/armeabi-v7a/libjpgt.so

▶ Show all **127** strings

lib/armeabi-v7a/liblept.so

▶ Show all **4164** strings

lib/armeabi-v7a/libpngt.so

▶ Show all **69** strings

lib/armeabi-v7a/libtess.so

▶ Show all **1937** strings

lib/armeabi-v7a/libTfaAndroid.so

▶ Show all **542** strings

ACTIVITIES

▶ Show all **180** activities

SERVICES

▼ Showing all **13** services

com.handelsbanken.android.resources.push.SHBFirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.analytics.AnalyticsService
com.google.android.gms.analytics.AnalyticsJobService
com.google.android.gms.tagmanager.TagManagerService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
androidx.room.MultiInstanceInvalidationService
org.acra.sender.LegacySenderService
org.acra.sender.JobSenderService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **4** receivers

com.google.android.gms.analytics.AnalyticsReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

PROVIDERS

▼ Showing all **5** providers

com.handelsbanken.android.resources.utils.PdfProvider
com.handelsbanken.android.resources.utils.ImageProvider

com.google.firebase.provider.FirebaseInitProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer
org.acra.attachment.AcraContentProvider

LIBRARIES

▼ Showing all **1** libraries
org.apache.http.legacy

SBOM

▼ Showing all **67** Versioned Packages
androidx.activity:activity-ktx@1.1.0
androidx.activity:activity@1.1.0
androidx.annotation:annotation-experimental@1.0.0
androidx.appcompat:appcompat-resources@1.2.0
androidx.appcompat:appcompat@1.2.0
androidx.arch.core:core-runtime@2.1.0
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.3.2
androidx.core:core@1.3.2
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@3.6.4
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.1
androidx.dynamicanimation:dynamicanimation@1.0.0
androidx.exifinterface:exifinterface@1.3.2
androidx.fragment:fragment-ktx@1.2.5
androidx.fragment:fragment@1.2.5
androidx.gridlayout:gridlayout@1.0.0
androidx.interpolator:interpolator@1.0.0

androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-extensions@2.2.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.2.0
androidx.lifecycle:lifecycle-livedata-core@2.2.0
androidx.lifecycle:lifecycle-livedata-ktx@2.2.0
androidx.lifecycle:lifecycle-livedata@2.2.0
androidx.lifecycle:lifecycle-process@2.2.0
androidx.lifecycle:lifecycle-runtime-ktx@2.2.0
androidx.lifecycle:lifecycle-runtime@2.2.0
androidx.lifecycle:lifecycle-service@2.2.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.2.0
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.2.0
androidx.lifecycle:lifecycle-viewmodel@2.2.0
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.navigation:navigation-common-ktx@2.3.2
androidx.navigation:navigation-common@2.3.2
androidx.navigation:navigation-fragment-ktx@2.3.2
androidx.navigation:navigation-fragment@2.3.2
androidx.navigation:navigation-runtime-ktx@2.3.2
androidx.navigation:navigation-runtime@2.3.2
androidx.navigation:navigation-ui-ktx@2.3.2
androidx.navigation:navigation-ui@2.3.2
androidx.percentlayout:percentlayout@1.0.0
androidx.preference:preference-ktx@1.1.1
androidx.preference:preference@1.1.1
androidx.print:print@1.0.0
androidx.recyclerview:recyclerview@1.1.0
androidx.room:room-runtime@2.2.5
androidx.savedstate:savedstate@1.0.0
androidx.slidingpanelayout:slidingpanelayout@1.0.0
androidx.sqlite:sqlite-framework@2.0.1
androidx.sqlite:sqlite@2.0.1
androidx.swiperefreshlayout:swiperefreshlayout@1.1.0

androidx.transition:transition@1.3.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.0
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0
androidx.webkit:webkit@1.4.0
com.google.android.material:material@1.3.0-rc01

▶ Show all **110** Packages

FILES

▶ Show all **8721** files

Version v4.3.0