ANDROID STATIC ANALYSIS REPORT

DAPNET (1.1.0)

File Name:	installer68.apk
Package Name:	de.hampager.dapnetmobile
Scan Date:	May 31, 2022, 1:56 p.m.
App Security Score:	**60/100 (LOW RISK)**
Grade:	**A**

FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	6	1	2	1

FILE INFORMATION

File Name: installer68.apk
Size: 3.4MB
MD5: e5aa74975a61094a50efda1a8f34b47e
SHA1: bcf372ea771ab0b17a8a2bc72c88f3d85d2c1cea
SHA256: b92b2c1cf466dbf5fdd0ab7ca5c6d38afd6e2211d09049738ddd6ab34ab67a28

APP INFORMATION

App Name: DAPNET
Package Name: de.hampager.dapnetmobile
Main Activity: de.hampager.dapnetmobile.activites.MainActivity
Target SDK: 27
Min SDK: 15
Max SDK:
Android Version Name: 1.1.0
Android Version Code: 22

■■ APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

✹ CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-05-20 22:01:23+00:00
Valid To: 2044-10-05 22:01:23+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x135d6f20
Hash Algorithm: sha256
md5: cc9fd4b5988bcf17bb2cfee05dbf4840
sha1: 3fe4d609790620596fdb23ac5b0ba28aed874166
sha256: f3bd72be60bd04aea13cc94a499ce7d4e67a0138aaa74f1c152088a7d872a4d1
sha512: fbf5007efccf3daeee07a15e9537156b52d44d99330c4768f0b14ba2806fecafad382e941f6e9467398462b16a3c15cd9b8f52294e8e8b8dd9c8a0adf25017d7

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

🔍 MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Activity (de.hampager.dapnetmobile.activites.LoginActivity) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/osmdroid/bonuspack/kml/IconStyle.java org/osmdroid/views/overlay/mylocation/GpsMyLocationProvider.java org/osmdroid/bonuspack/utils/WebImageCache.java org/osmdroid/tileprovider/modules/MapTileDownloader.java org/osmdroid/bonuspack/routing/GraphHopperRoadManager.java org/osmdroid/config/DefaultConfigurationProvider.java de/hampager/dapnetmobile/activites/MainActivity.java org/osmdroid/tileprovider/util/Counters.java de/hampager/dapnetmobile/adapters/RubricAdapter.java de/hampager/dapnetmobile/adapters/NodeAdapter.java org/osmdroid/views/overlay/TilesOve

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/osmdroid/views/overlay/TilesOverlay.java
				com/tokenautocomplete/TokenCompleteTextView.java
				org/osmdroid/bonuspack/location/GeocoderNominatim.java
				org/metalev/multitouch/controller/MultiTouchController.java
				org/osmdroid/tileprovider/modules/DatabaseFileArchive.java
				org/osmdroid/tileprovider/modules/SqliteArchiveTileWriter.java
				org/osmdroid/views/overlay/DefaultOverlayManager.java
				org/osmdroid/bonuspack/utils/HttpConnection.java
				org/osmdroid/tileprovider/modules/OfflineTileProvider.java
				org/osmdroid/bonuspack/location/GeoNamesPOIProvider.java
				org/osmdroid/tileprovider/tilesource/bing/BingMapTileSource.java
				org/osmdroid/tileprovider/modules/MapTileSqlCacheProvider.java
				org/osmdroid/tileprovider/MapTileCache.java
				org/osmdroid/tileprovider/modules/GEMFFileArchive.java
				de/hampager/dapnetmobile/adapters/RubricContentAdapter.java
				org/osmdroid/views/overlay/infowindow/BasicInfoWindow.java
				de/hampager/dapnetmobile/fragments/TableFragment.java
				org/osmdroid/tileprovider/util/StorageUtils.java
				org/osmdroid/bonuspack/kml/KmlDocument.java
				org/osmdroid/tileprovider/BitmapPool.java
				org/osmdroid/bonuspack/routing/OSRMRoadManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				RMRoadManager.java org/osmdroid/views/overlay/NonAcceleratedOverlay.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	org/osmdroid/tileprovider/modules/ArchiveFileFactory.java de/hampager/dapnetmobile/fragments/WelcomeFragment.java org/osmdroid/views/overlay/gridlines/LatLonGridlineOverlay.java org/osmdroid/tileprovider/modules/TileWriter.java org/osmdroid/tileprovider/modules/MapTileModuleProviderBase.java org/osmdroid/bonuspack/routing/RoadLeg.java org/osmdroid/tileprovider/LRUMapTileCache.java org/osmdroid/bonuspack/routing/MapQuestRoadManager.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/osmdroid/tileprovider/modules/MapTileFileArchiveProvider.java org/osmdroid/tileprovider/modules/MapTileFilesystemProvider.java org/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.java de/hampager/dapnetmobile/fragments/CallFragment.java org/osmdroid/bonuspack/routing/Road.java de/hampager/dapnetmobile/adapters/SubscriberAdapter.java org/osmdroid/tileprovider/util/ManifestUtil.java org/osmdroid/bonuspack/routing/GoogleRoadManager.java org/osmdroid/bonuspack/location/FlickrPOIProvider.java org/osmdroid/bonuspack/routing/MapQuestRoadManagerV1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/osmdroid/bonuspack/location/OverpassAPIProvider.java org/osmdroid/views/overlay/infowindow/InfoWindow.java org/osmdroid/tileprovider/util/CloudmadeUtil.java org/osmdroid/tileprovider/modules/ZipFileArchive.java org/osmdroid/views/overlay/mylocation/MyLocationNewOverlay.java de/hampager/dapnetmobile/activites/PostCallActivity.java de/hampager/dapnetmobile/fragments/MapFragment.java org/osmdroid/views/overlay/infowindow/MarkerInfoWindow.java org/osmdroid/bonuspack/location/NominatimPOIProvider.java org/osmdroid/tileprovider/modules/TileDownloader.java org/osmdroid/tileprovider/cachemanager/CacheManager.java org/osmdroid/views/MapView.java org/osmdroid/events/DelayedMapListener.java org/osmdroid/tileprovider/tilesource/CloudmadeTileSource.java de/hampager/dapnetmobile/adapters/CallAdapter.java org/osmdroid/tileprovider/modules/MBTilesFileArchive.java de/hampager/dapnetmobile/activites/LoginActivity.java org/osmdroid/tileprovider/MapTileProviderBase.java org/osmdroid/bonuspack/location/PicasaPOIProvider.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	org/osmdroid/bonuspack/location/GeocoderNominatim.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/tilesource/bing/BingMapTileSource.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/osmdroid/tileprovider/util/CloudmadeUtil.java
3	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	org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/modules/SqliteArchiveTileWriter.java org/osmdroid/tileprovider/modules/SqlTileWriter.java
4	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	org/osmdroid/tileprovider/util/StorageUtils.java org/osmdroid/bonuspack/kml/KmlDocument.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	de/hampager/dap4j/ServiceGenerator.java
6	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	org/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.java

🔳 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no 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 generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
11	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.
12	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.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.opengis.net	ok	**IP:** 66.244.86.70 **Country:** United States of America **Region:** Indiana **City:** Jasper **Latitude:** 38.391441 **Longitude:** -86.931107 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.geonames.org	ok	**IP:** 176.9.107.169 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
b.tile.thunderforest.com	ok	**IP:** 88.99.99.5 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map
graphhopper.com	ok	**IP:** 5.9.203.233 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
b.tile.openstreetmap.org	ok	**IP:** 151.101.38.137 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
c.tiles.wmflabs.org	ok	**IP:** 185.15.56.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** [Google Map](#)
wms.chartbundle.com	ok	**IP:** 138.68.60.210 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** [Google Map](#)
opentopomap.org	ok	**IP:** 131.188.76.144 **Country:** Germany **Region:** Bayern **City:** Erlangen **Latitude:** 49.595612 **Longitude:** 10.994970 **View:** [Google Map](#)
schemas.google.com	ok	No Geolocation information available.
a.tile.openstreetmap.org	ok	**IP:** 151.101.38.137 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
a.tile.thunderforest.com	ok	IP: 88.99.98.237 Country: Germany Region: Bayern City: Gunzenhausen Latitude: 48.323330 Longitude: 11.601220 View: [Google Map](#)
router.project-osrm.org	ok	IP: 88.99.61.41 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: [Google Map](#)
1.domain	ok	No Geolocation information available.
auth.cloudmade.com	ok	IP: 23.21.136.107 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: [Google Map](#)
api.openstreetmap.fr	ok	IP: 164.132.171.101 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
3.domain	ok	No Geolocation information available.
www.afu.rwth-aachen.de	ok	**IP:** 137.226.79.98 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Aachen **Latitude:** 50.776642 **Longitude:** 6.083420 **View:** [Google Map](#)
overlay.openstreetmap.nl	ok	**IP:** 93.186.176.173 **Country:** Netherlands **Region:** Overijssel **City:** Enschede **Latitude:** 52.218330 **Longitude:** 6.895830 **View:** [Google Map](#)
api.flickr.com	ok	**IP:** 108.156.66.73 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** [Google Map](#)
overpass-api.de	ok	**IP:** 178.63.48.217 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
hampager.de	ok	IP: 137.226.79.98 Country: Germany Region: Nordrhein-Westfalen City: Aachen Latitude: 50.776642 Longitude: 6.083420 View: Google Map
www.flickr.com	ok	IP: 108.156.66.73 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.hampager.de	ok	IP: 137.226.79.98 Country: Germany Region: Nordrhein-Westfalen City: Aachen Latitude: 50.776642 Longitude: 6.083420 View: Google Map
tiles.openseamap.org	ok	IP: 195.37.132.70 Country: Germany Region: Rheinland-Pfalz City: Franken Latitude: 50.501240 Longitude: 7.234600 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.tiles.mapbox.com	ok	**IP:** 18.65.34.184 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
picasaweb.google.com	ok	**IP:** 172.217.168.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
db0sda.ampr.org	ok	**IP:** 44.149.166.2 **Country:** United States of America **Region:** California **City:** San Diego **Latitude:** 32.800457 **Longitude:** -117.171066 **View:** [Google Map](#)
b.tile.cloudmade.com	ok	No Geolocation information available.
2.domain	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
basemap.nationalmap.gov	ok	**IP:** 65.9.85.78 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** [Google Map](#)
maps.googleapis.com	ok	**IP:** 172.217.168.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** [Google Map](#)
c.tile.thunderforest.com	ok	**IP:** 88.99.98.237 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** [Google Map](#)
a.tile.cloudmade.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
open.mapquestapi.com	ok	IP: 34.237.118.100 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
www.google.com	ok	IP: 142.250.179.164 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
a.tiles.wmflabs.org	ok	IP: 185.15.56.55 Country: United States of America Region: California City: San Francisco Latitude: 37.788464 Longitude: -122.394608 View: Google Map
c.tile.openstreetmap.org	ok	IP: 151.101.38.137 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
dev.virtualearth.net	ok	**IP:** 52.156.193.145 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** [Google Map](#)
b.tiles.wmflabs.org	ok	**IP:** 185.15.56.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** [Google Map](#)
openptmap.org	ok	**IP:** 88.99.141.112 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** [Google Map](#)
nominatim.openstreetmap.org	ok	**IP:** 130.117.76.9 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** [Google Map](#)
c.tile.cloudmade.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
4.domain	ok	No Geolocation information available.

Report Generated by - MobSF v3.5.2 Beta

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