MOBSF

ANDROID STATIC ANALYSIS REPORT

Timber (1.6.1)

File Name:	timber.apk
Package Name:	it.fossoft.timberfoss
Average CVSS Score:	5.9
App Security Score:	10/100 (CRITICAL RISK)

FILE INFORMATION

File Name: timber.apk
Size: 7.71MB
MD5: a317272507314b4c4197d6733c5ab725
SHA1: 54aa3980add31470fcac1e069b32bf3ef155a665
SHA256: 380978bb333d2d75496a90cc5252e07f084f95e9f87bea59ed60b1686531a80f

APP INFORMATION

App Name: Timber
Package Name: it.fossoft.timberfoss
Main Activity: com.naman14.timber.activities.MainActivity
Target SDK: 27
Min SDK: 16
Max SDK:
Android Version Name: 1.6.1
Android Version Code: 21

APP COMPONENTS

Activities: 7
Services: 2
Receivers: 4
Providers: 0
Exported Activities: 0
Exported Services: 1
Exported Receivers: 4
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: 2019-05-05 13:36:28+00:00
Valid To: 2046-09-20 13:36:28+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x111ece28
Hash Algorithm: sha256
md5: 02ed5e71589c0294257a110c00c3e2fd
sha1: f9d809236fe1f392528679de80a2effefe93727e
sha256: d3fac661c376198df7d842b45cb57c49726149c4edb01c872efb4aff9ac22e01
sha512:
1a93cf668a3624b84f08890d83f46f523eb93b28461179ae9a1cac3e2974d813b4ac9330b6b9a9bcfd9dede0c17516c41cd77e75d0491cfc90ad71206be8bbce

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
com.android.vending.BILLING	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti-VM Code: Build.FINGERPRINT check Build.MANUFACTURER check Compiler: dx

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.naman14.timber.activities.MainActivity	Schemes: file://, http://, content://, Mime Types: audio/*, application/ogg, application/x-ogg, application/itunes,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.naman14.timber.helpers.MediaButtonIntentReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Service (com.naman14.timber.WearBrowserService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Broadcast Receiver (com.naman14.timber.widgets.desktop.StandardWidget) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.naman14.timber.widgets.desktop.WhiteWidget) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.naman14.timber.widgets.desktop.SmallWidget) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 - Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/afollestad/appthemeengine/ConfigBase.java com/anjlab/android/iab/v3/BillingCache.java com/anjlab/android/iab/v3/BillingProcessor.java com/naman14/timber/lastfmapi/LastFmClient.java com/naman14/timber/lastfmapi/models/LastfmUserSession.java
			com/afollestad/appthemeengine/processors/DefaultProcessor.java com/afollestad/appthemeengine/processors/TabLayoutProcessor.java com/afollestad/materialdialogs/MaterialDialog.java com/anjlab/android/iab/v3/SkuDetails.java com/anjlab/android/iab/v3/TransactionDetails.java com/naman14/timber/activities/PlaylistDetailActivity.java

This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	com/naman14/timber/fragments/SettingsFragment.java com/naman14/timber/utils/LyricsExtractor.java com/naman14/timber/utils/NavigationUtils.java com/nostra13/universalimageloader/cache/disc/naming/HashCodeFileNameGenerator.java com/nostra13/universalimageloader/core/imageaware/NonViewAware.java com/nostra13/universalimageloader/core/imageaware/ViewAware.java retrofit/Types.java retrofit/client/Header.java retrofit/mime/TypedByteArray.java retrofit/mime/TypedFile.java
IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor OWASP MASVS: MSTG-CODE-2	com/afollestad/materialdialogs/BuildConfig.java com/afollestad/materialdialogs/commons/BuildConfig.java fi/iki/elonen/NanoHTTPD.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/afollestad/materialdialogs/folderselector/FileChooserDialog.java com/afollestad/materialdialogs/folderselector/FolderChooserDialog.java com/naman14/timber/dialogs/StorageSelectDialog.java com/naman14/timber/utils/PreferencesUtility.java com/nostra13/universalimageloader/utils/StorageUtils.java
The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/anjlab/android/iab/v3/BillingProcessor.java com/anjlab/android/iab/v3/PurchaseInfo.java com/anjlab/android/iab/v3/Security.java com/naman14/timber/MusicService.java com/naman14/timber/activities/PlaylistDetailActivity.java com/naman14/timber/adapters/PlayingQueueAdapter.java com/naman14/timber/dataloaders/NowPlayingCursor.java com/naman14/timber/fragments/QueueFragment.java com/naman14/timber/lastfmapi/LastFmClient.java com/naman14/timber/nowplaying/BaseNowplayingFragment.java com/naman14/timber/utils/TimberUtils.java com/naman14/timber/widgets/DragSortRecycler.java com/naman14/timber/widgets/PlayPauseDrawable.java fi/iki/elonen/util/ServerRunner.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java retrofit/Platform.java

			retrofit/android/AndroidLog.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/naman14/timber/MusicService.java com/naman14/timber/adapters/PlaylistAdapter.java com/naman14/timber/permissions/PermissionRequest.java com/naman14/timber/subfragments/PlaylistPagerFragment.java com/naman14/timber/widgets/MusicVisualizer.java
MD5 is a weak hash known to have hash collisions.	high	CVSS V2: 7.4 (high) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/naman14/timber/lastfmapi/LastFmClient.java okio/Buffer.java
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.	high	CVSS V2: 5.9 (medium) CWE: CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/naman14/timber/provider/MusicPlaybackState.java com/naman14/timber/provider/RecentStore.java com/naman14/timber/provider/SearchHistory.java com/naman14/timber/provider/SongPlayCount.java
App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fi/iki/elonen/NanoHTTPD.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	good	IP: 13.234.210.38 Country: India Region: Maharashtra City: Mumbai Latitude: 19.01441 Longitude: 72.847939 View: Google Map
ws.audioscrobbler.com	good	IP: 64.30.224.206 Country: United States of America Region: Florida City: Fort Lauderdale Latitude: 26.183096 Longitude: -80.173927 View: Google Map
makeitpersonal.co	good	IP: 107.170.105.41 Country: United States of America Region: New York City: New York City Latitude: 40.719936 Longitude: -74.005013

		View: Google Map
plus.google.com	good	IP: 172.217.166.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
schemas.android.com	good	No Geolocation information available.
twitter.com	good	IP: 104.244.42.193 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map

URLS

URL	FILE
http://schemas.android.com/apk/res/android	com/afollestad/materialdialogs/prefs/PrefUtil.java
http://ws.audioscrobbler.com/2.0 https://ws.audioscrobbler.com/2.0	com/naman14/timber/lastfmapi/LastFmClient.java
https://plus.google.com/communities/111029425713454201429 https://github.com/naman14 https://plus.google.com/u/0/+NamanDwivedi14 https://github.com/naman14/Timber/issues https://twitter.com/naman1405	com/naman14/timber/utils/Helpers.java
https://makeitpersonal.co	com/naman14/timber/utils/LyricsLoader.java

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM

71 - 100	LOW

Report Generated by - MobSF v3.0.9 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.