MOBSF

ANDROID STATIC ANALYSIS REPORT

Aegis-2.2.2.zip

File Name:	Aegis-2.2.2.zip
Package Name:	
Scan Date:	Oct. 6, 2023, 3:13 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	7	2	2	0

FILE INFORMATION

File Name: Aegis-2.2.2.zip
Size: 7.83MB
MD5: 24b001ebc8bd1a0f9d577690b4b00d46
SHA1: 25da20967b6b266c5c823292a276b6043a904ce8
SHA256: 6554fb72d992bcb84a7ec158c3b81acc7cb2528114c24c7124618eae9e43d54d

APP INFORMATION

App Name:
Package Name:
Main Activity:
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 12
Services: 2
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
	unknown	Unknown permission	Unknown permission from android reference

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

CODE ANALYSIS

HIGH: 2 | WARNING: 5 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/beemdevelopment/aegis/ui/AboutActivity.java com/beemdevelopment/aegis/ui/MainActivity.java com/beemdevelopment/aegis/ui/TransferEntriesActivity.java com/beemdevelopment/aegis/ui/dialogs/Dialogs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Hidden elements in view can be used to hide data from user. But this data can be leaked	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-STORAGE-7	com/beemdevelopment/aegis/helpers/FabScrollHelper.java com/beemdevelopment/aegis/ui/AuthActivity.java com/beemdevelopment/aegis/ui/EditEntryActivity.java com/beemdevelopment/aegis/ui/GroupManagerActivity.java com/beemdevelopment/aegis/ui/MainActivity.java com/beemdevelopment/aegis/ui/TransferEntriesActivity.java com/beemdevelopment/aegis/ui/dialogs/Dialogs.java com/beemdevelopment/aegis/ui/fragments/preferences/IconPacksManagerFragment.java com/beemdevelopment/aegis/ui/views/EntryHolder.java com/beemdevelopment/aegis/ui/views/EntryListView.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/beemdevelopment/aegis/importers/SqlImporterHelper.java com/beemdevelopment/aegis/ui/fragments/preferences/ImportExportPreferencesFragment.java com/beemdevelopment/aegis/ui/tasks/ImportFileTask.java com/beemdevelopment/aegis/ui/tasks/ImportIconPackTask.java com/beemdevelopment/aegis/vault/VaultManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App has capabilities to prevent against Screenshots from Recent Task History/ Now On Tap etc.	secure	OWASP MASVS: MSTG-STORAGE-9	com/beemdevelopment/aegis/ui/AegisActivity.java com/beemdevelopment/aegis/ui/dialogs/Dialogs.java
5	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/beemdevelopment/aegis/importers/AuthenticatorProImporter.java com/beemdevelopment/aegis/importers/AuthyImporter.java com/beemdevelopment/aegis/importers/TotpAuthenticatorImporter.java
6	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/beemdevelopment/aegis/importers/AuthyImporter.java
7	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/beemdevelopment/aegis/AegisBackupAgent.java com/beemdevelopment/aegis/helpers/QrCodeAnalyzer.java com/beemdevelopment/aegis/vault/VaultBackupManager.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/beemdevelopment/aegis/importers/SqlImporterHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	com/beemdevelopment/aegis/Preferences.java com/beemdevelopment/aegis/importers/TotpAuthenticatorImporter.java
10	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/beemdevelopment/aegis/ui/fragments/preferences/ImportExportPreferencesFragment.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

EMAILS

EMAIL	FILE
beemdevelopment@gmail.com	com/beemdevelopment/aegis/ui/AboutActivity.java

HARDCODED SECRETS

POSSIBLE SECRETS
927f7e38b6acbecd84e02dace33efa9a7a2f0979750f28f585688ee38b3a4e28
23456789BCDFGHJKMNPQRTVWXY
398e27fc50276a656065b0e525f4c06c04c61075286b8e7aeda59da9813b5dd6c80d2fb38068773fa59ba47c17ca6c6479015c1d5b8b8f6b9a

---

Report Generated by - MobSF v3.7.8 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.