ANDROID STATIC ANALYSIS REPORT

app_icon

Hallowed (1.0)

File Name:	app-docker.apk
Package Name:	com.ecw2022.hallowed
Scan Date:	Nov. 3, 2022, 9:39 a.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
0	6	1	1	0

FILE INFORMATION

File Name: app-docker.apk
Size: 5.73MB
MD5: 75484fb8c2fa11f80b8903aedbbd7d9b
SHA1: 8e59336bd2d82ed1ca4510cf0d16703ee83fcfde
SHA256: 09af132859a4eb7bb0dce9ac906072b727226ef2df03a76f20c07a7917aa01ab

APP INFORMATION

App Name: Hallowed
Package Name: com.ecw2022.hallowed
Main Activity: com.ecw2022.hallowed.MainActivity
Target SDK: 32
Min SDK: 30
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 4
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 3
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=test
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-08-18 13:15:18+00:00
Valid To: 2047-08-12 13:15:18+00:00
Issuer: CN=test
Serial Number: 0x395220d4
Hash Algorithm: sha256
md5: 5a9de53ef7e2dc4d3c0e78954c9e05e7
sha1: 5ca636d36e1b803da9ebf1532b58db828ffc4f4c
sha256: e16f30219338a76230e7de14e958a70acc7d0bb4ee6f5369d29c73d6e56a816e
sha512: 13ac2793d74199d310c4bde9a618b5671c6d5525d0b079be84433039ca64496e9c0aa7702e4503566ff666482e93e17c76b0e18806312dff459edbbfe8fcb425
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8547dde98ba4fe9d4c91ce4f9a080b4cd7337b75814aa17689171320a0919832
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.ecw2022.WHAT_A_FUNNY_PERM	unknown	Unknown permission	Unknown permission from android reference
com.ecw2022.ACCESS_LOCATION	unknown	Unknown permission	Unknown permission from android reference
com.ecw2022.I_SEE_YOU	unknown	Unknown permission	Unknown permission from android reference
com.ecw2022.ADMIN_PERM_D0_N0T_ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.ecw2022.USER_PERM	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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 (com.ecw2022.hallowed.FunnyActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.ecw2022.WHAT_A_FUNNY_PERM protectionLevel: dangerous [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. It is protected by a permission. However, the protection level of the permission is set to dangerous. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (com.ecw2022.hallowed.UserActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.ecw2022.USER_PERM protectionLevel: normal [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. It is protected by a permission. However, the protection level of the permission is set to normal. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
4	Activity (com.ecw2022.hallowed.AdminActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.ecw2022.ADMIN_PERM_D0_N0T_ACCESS [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. 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/ecw2022/hallowed/FunnyActivity.java
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	com/ecw2022/hallowed/AdminActivity.java com/ecw2022/hallowed/MainActivity.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 no hardware resources.
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 no 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.

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"username" : "Email"

Report Generated by - MobSF v3.6.1 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.