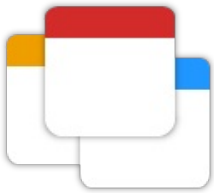
# ANDROID STATIC ANALYSIS REPORT



## Small Apps Manager (3.4.A.0.0)

| | |
|---|---|
| File Name: | s/com.sony.smallapp.managerservice_3.4.A.0.0-6815744_minAPI24(nodpi)_apkmirror.com.apk |
| Package Name: | com.sony.smallapp.managerservice |
| Average CVSS Score: | 5.7 |
| App Security Score: | 75/100 (LOW RISK) |
| Trackers Detection: | 1/320 |

# FILE INFORMATION

**File Name:** s/com.sony.smallapp.managerservice_3.4.A.0.0-6815744_minAPI24(nodpi)_apkmirror.com.apk
**Size:** 0.29MB
**MD5:** dd286fe7ddac3040e9f7e2b965ebe7e2
**SHA1:** 1474a6bb34d57040736c6be0a336d6ae550e3cd7
**SHA256:** fa7bc4623c870511ae6cf3dbce4be51ecd33a9a4b74e6e35c9626c48cc869422

# APP INFORMATION

**App Name:** Small Apps Manager
**Package Name:** com.sony.smallapp.managerservice
**Main Activity:**
**Target SDK:** 24
**Min SDK:** 24
**Max SDK:**
**Android Version Name:** 3.4.A.0.0
**Android Version Code:** 6815744

# APP COMPONENTS

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

# CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=SE, O=Sony Ericsson Mobile Communications AB, CN=Sony_Ericsson_E_Platform_Signing_Live_864f
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2000-01-01 14:10:18+00:00
Valid To: 2035-01-01 14:10:18+00:00
Issuer: C=SE, O=Sony Ericsson Mobile Communications AB, CN=Sony_Ericsson_E_CA_Live_864f
Serial Number: 0x3
Hash Algorithm: sha1
md5: 9e5b0111e0408bb405c819ea0784b69d
sha1: 80d0156e14efa9b2be949acc1791720cc58cb6e3
sha256: 6339375ac295cb0cd22811b97accd40104bd4a0185d4dd2289b81860c15d623c
sha512:

0b465d828ecf42f1a6cec997fb953dad6b6fdb36193942d4a3297053ed42a4e27fa3d1128963a5083a3ac34312991a4d9e8772a02253d9ba4d46b3b28d750df6

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 78e421a9a208b628c5e7383023f140a3c74417dde0a6b06eb249af4f01af7d24

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

# APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| com.sony.smallapp.permission.POLICY_CONTROL | dangerous | Unknown permission from android reference | Unknown permission from android reference |
| com.sony.smallapp.permission.SMALLAPPMANAGER_CONTROL | dangerous | Unknown permission from android reference | Unknown permission from android reference |
| com.sony.smallapp.permission.CONTROL_SMALLAPP | dangerous | Unknown permission from android reference | Unknown permission from android reference |
| 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.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.EXPAND_STATUS_BAR | normal | expand/collapse status bar | Allows application to expand or collapse the status bar. |
| com.sony.smallapp.permission.SMALLAPP | dangerous | Unknown permission from android reference | Unknown permission from android reference |

# APKID ANALYSIS

| FILE | DETAILS |
|---|---|
| classes.dex | FINDINGS: Compiler — DETAILS: dx (possible dexmerge)<br>FINDINGS: Manipulator Found — DETAILS: dexmerge |

# MANIFEST ANALYSIS

| ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|
| Service (com.sony.smallapp.managerservice.SmallAppManagerService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.sony.smallapp.permission.SMALLAPPMANAGER_CONTROL<br>protectionLevel: signatureOrSystem<br>[android:exported=true] | info | A Service is found to be exported, but is protected by a permission. However, the protection level of the permission is set to signatureOrSystem. It is recommended that signature level is used instead. Signature level should suffice for most purposes, and does not depend on where the applications are installed on the device. |
| Service (com.sony.smallapp.managerservice.SmallAppManagerInterfaceService) is not Protected.<br>[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. |
| Service (com.sony.smallapp.managerservice.PolicyManagerService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.sony.smallapp.permission.POLICY_CONTROL<br>protectionLevel: signatureOrSystem<br>[android:exported=true] | info | A Service is found to be exported, but is protected by a permission. However, the protection level of the permission is set to signatureOrSystem. It is recommended that signature level is used instead. Signature level should suffice for most purposes, and does not depend on where the applications are installed on the device. |

# </> CODE ANALYSIS

| ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|
| 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)<br>**CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm<br>**OWASP MASVS:** MSTG-CRYPTO-4 | com/sony/smallapp/managerservice/SmallAppManagerService.java |
| The App logs information. Sensitive information should never be logged. | info | **CVSS V2:** 7.5 (high)<br>**CWE:** CWE-532 - Insertion of Sensitive Information into Log File<br>**OWASP MASVS:** MSTG-STORAGE-3 | com/sony/smallapp/managerservice/Utils.java<br>com/sonymobile/gahelper/GaHelperExceptionParser.java<br>com/sonymobile/gahelper/GaHelperSubscriber.java<br>com/sonymobile/gahelper/GaHelperLog.java<br>com/sonymobile/gahelper/GaHelper.java |
| Files may contain hardcoded sensitive informations like usernames, passwords, keys etc. | high | **CVSS V2:** 7.4 (high)<br>**CWE:** CWE-312 - Cleartext Storage of Sensitive Information<br>**OWASP Top 10:** M9: Reverse Engineering<br>**OWASP MASVS:** MSTG-STORAGE-14 | com/sony/smallapp/managerservice/ConfirmLaunchController.java |

# TRACKERS

| TRACKER | URL |
|---|---|
| Google Analytics | https://reports.exodus-privacy.eu.org/trackers/48 |

## 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 v3.0.7 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.