ANDROID STATIC ANALYSIS REPORT

File Name:	sample.apk
Package Name:	com.jpdesigns.dashboardzooper
Scan Date:	Oct. 15, 2025, 3:19 a.m.
App Security Score:	34/100 (HIGH RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	1	0	1	0

FILE INFORMATION

File Name: sample.apk
Size: 0.38MB
MD5: 9150c54637f38c1dcf8a373c9d864db2
SHA1: e5e13f8a71f8b7b82d6b3c38a8f5c3928d57e060
SHA256: 6a97b47aafbb1c8b3312e43e40c5ce2d9c42cc45e234ebea3489cab0eb05acd9

APP INFORMATION

App Name: Sample
Package Name: com.jpdesigns.dashboardzooper
Main Activity:
Target SDK: 15
Min SDK: 15
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

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

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: O=J P Designs
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-12-07 02:50:11+00:00
Valid To: 2063-11-25 02:50:11+00:00
Issuer: O=J P Designs
Serial Number: 0x5eb43a4d
Hash Algorithm: sha256
md5: aeb1785af5f9943bf9ddf17917df5ab8
sha1: eeacc72449562188e8ea0668c5e56f37e93f38fe
sha256: 609d1b26ab681b36483591fea1874c21f9be3b2081ba63d0447922f1c1cac2cc
sha512: e03feb2693eba358062ab326a18bbf021abb7914259970ee74d14afa3e3c1d88d62224e2c95dd1d8aa33d1aadeb0be309d5df8fa5eee423d124cbcfbab954b82
Found 1 unique certificates

APKID ANALYSIS

FILE	DETAILS
classes.dex	

FINDINGS	DETAILS
Compiler	dx (possible dexmerge)
Manipulator Found	dexmerge

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.jpdesigns.dashboardzooper.ZooperTemplate) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (15) of the app to 29 or higher to fix this issue at platform level.
3	Activity (com.jpdesigns.dashboardzooper.ZooperTemplate) is not Protected. [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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/24	
Other Common Permissions	0/45	

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

HARDCODED SECRETS

POSSIBLE SECRETS

"zooper_pack_author" : "JPDesigns"

SCAN LOGS

Timestamp	Event	Error
2025-10-15 03:19:33	Generating Hashes	OK
2025-10-15 03:19:33	Extracting APK	OK
2025-10-15 03:19:33	Unzipping	OK
2025-10-15 03:19:33	Getting Hardcoded Certificates/Keystores	OK
2025-10-15 03:19:35	Parsing AndroidManifest.xml	OK
2025-10-15 03:19:35	Parsing APK with androguard	OK
2025-10-15 03:19:35	Extracting Manifest Data	OK
2025-10-15 03:19:35	Performing Static Analysis on: Sample (com.jpdesigns.dashboardzooper)	OK

2025-10-15 03:19:35	Fetching Details from Play Store: com.jpdesigns.dashboardzooper	OK
2025-10-15 03:19:36	Manifest Analysis Started	OK
2025-10-15 03:19:36	Checking for Malware Permissions	OK
2025-10-15 03:19:36	Fetching icon path	OK
2025-10-15 03:19:36	Library Binary Analysis Started	OK
2025-10-15 03:19:36	Reading Code Signing Certificate	OK
2025-10-15 03:19:37	Running APKiD 2.1.5	OK
2025-10-15 03:19:41	Detecting Trackers	OK
2025-10-15 03:19:42	Decompiling APK to Java with jadx	OK
2025-10-15 03:19:42	Converting DEX to Smali	OK
2025-10-15 03:19:42	Code Analysis Started on - java_source	OK
2025-10-15 03:19:42	Android SAST Completed	OK

2025-10-15 03:19:42	Android API Analysis Started	OK
2025-10-15 03:19:42	Finished Code Analysis, Email and URL Extraction	OK
2025-10-15 03:19:42	Extracting String data from APK	OK
2025-10-15 03:19:42	Extracting String data from Code	OK
2025-10-15 03:19:42	Extracting String values and entropies from Code	OK
2025-10-15 03:19:42	Performing Malware check on extracted domains	OK
2025-10-15 03:19:42	Saving to Database	OK

© 2025 | Android Static Analysis.