



ANDROID STATIC ANALYSIS REPORT



 00000000 (2.0)

File Name: 36f40d5a11d886a2280c57859cd5f22de2d78c87dcdb52ea601089745eeee494.apk

Package Name: com.android.tencent.zdevs.bah

Scan Date: April 27, 2025, 2:33 p.m.

App Security Score: **36/100 (HIGH RISK)**

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	2	0	1	1

FILE INFORMATION

File Name: 36f40d5a11d886a2280c57859cd5f22de2d78c87dcdb52ea601089745eeee494.apk

Size: 1.95MB

MD5: 8ce42ae8f1206130aeadaa7cad062aca

SHA1: ca2e7c66b9eedf95f51204cea8cd2e13ba2a5d93

SHA256: 36f40d5a11d886a2280c57859cd5f22de2d78c87dcdb52ea601089745eeee494

APP INFORMATION

App Name: □□□□□□□□

Package Name: com.android.tencent.zdevs.bah

Main Activity: com.android.tencent.zdevs.bah.MainActivity

Target SDK: 21

Min SDK: 14

Max SDK:

Android Version Name: 2.0

Android Version Code: 2

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: CN=873472648

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2017-01-04 12:01:10+00:00

Valid To: 2116-12-11 12:01:10+00:00

Issuer: CN=873472648

Serial Number: 0x1

Hash Algorithm: sha256

md5: 16d618041e99d60026921773e0cfcc41

sha1: 4752f7fb4f1d88427a3b2388ce061ca510b7c157

sha256: eaa9f05aeab23ec28bbc651205691722f29e9075a163a2e9d044a0d7f142fa37

sha512: ca2e152130c3ede4571a72383b5cf8ee1db826b46984582e889ace91d165e41bfbfd8db126954128fd12c6cab03ef261f6872d4c32a109ef2a785ac7f3cf3d8

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_CONFIGURATION	SignatureOrSystem	change your UI settings	Allows an application to change the current configuration, such as the locale or overall font size.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	dexlib 1.x

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: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0-4.0.2, [minSdk=14]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	Activity-Alias (com.android.tencent.zdevs.bah.QQ1279525738) is not Protected. An intent-filter exists.	warning	An Activity-Alias 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 Activity-Alias is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

👤 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

🔗 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
------	---------	-------------

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.SET_WALLPAPER, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.GET_TASKS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	1/44	android.permission.MODIFY_AUDIO_SETTINGS

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
--------	----------------

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.styleseven.comfreeware	ok	No Geolocation information available.
www.styleseven.comlight	ok	No Geolocation information available.

 SCAN LOGS

Timestamp	Event	Error
2025-04-27 14:33:17	Generating Hashes	OK
2025-04-27 14:33:17	Extracting APK	OK
2025-04-27 14:33:17	Unzipping	OK
2025-04-27 14:33:17	Parsing APK with androguard	OK
2025-04-27 14:33:18	Extracting APK features using aapt/aapt2	OK
2025-04-27 14:33:18	Getting Hardcoded Certificates/Keystores	OK
2025-04-27 14:33:19	Parsing AndroidManifest.xml	OK
2025-04-27 14:33:19	Extracting Manifest Data	OK
2025-04-27 14:33:19	Manifest Analysis Started	OK

2025-04-27 14:33:19	Performing Static Analysis on: ██████████ (com.android.tencent.zdevs.bah)	OK
2025-04-27 14:33:19	Fetching Details from Play Store: com.android.tencent.zdevs.bah	OK
2025-04-27 14:33:19	Checking for Malware Permissions	OK
2025-04-27 14:33:19	Fetching icon path	OK
2025-04-27 14:33:19	Library Binary Analysis Started	OK
2025-04-27 14:33:19	Analyzing assets/ssspbahk.so	OK
2025-04-27 14:33:19	Analyzing apktool_out/assets/ssspbahk.so	OK
2025-04-27 14:33:19	Reading Code Signing Certificate	OK
2025-04-27 14:33:19	Running APKiD 2.1.5	OK
2025-04-27 14:33:20	Detecting Trackers	OK
2025-04-27 14:33:21	Decompiling APK to Java with JADX	OK

2025-04-27 14:33:23	Converting DEX to Smali	OK
2025-04-27 14:33:23	Code Analysis Started on - java_source	OK
2025-04-27 14:33:24	Android SBOM Analysis Completed	OK
2025-04-27 14:33:24	Android SAST Completed	OK
2025-04-27 14:33:24	Android API Analysis Started	OK
2025-04-27 14:33:24	Android API Analysis Completed	OK
2025-04-27 14:33:24	Android Permission Mapping Started	OK
2025-04-27 14:33:25	Android Permission Mapping Completed	OK
2025-04-27 14:33:25	Android Behaviour Analysis Started	OK
2025-04-27 14:33:25	Android Behaviour Analysis Completed	OK
2025-04-27 14:33:25	Extracting Emails and URLs from Source Code	OK

2025-04-27 14:33:25	Email and URL Extraction Completed	OK
2025-04-27 14:33:25	Extracting String data from APK	OK
2025-04-27 14:33:25	Extracting String data from SO	OK
2025-04-27 14:33:25	Extracting String data from Code	OK
2025-04-27 14:33:25	Extracting String values and entropies from Code	OK
2025-04-27 14:33:25	Performing Malware check on extracted domains	OK
2025-04-27 14:33:26	Saving to Database	OK

Report Generated by - MobSF v4.3.2

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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).