ANDROID STATIC ANALYSIS REPORT

No icon

@string/app_name_prod

File Name:	apps-android-wikipedia-r-2.7.50452-r-2023-09-06.zip
Package Name:	
Scan Date:	Oct. 6, 2023, 2:47 p.m.
App Security Score:	**62/100 (LOW RISK)**
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	4	2	2	1

FILE INFORMATION

File Name: apps-android-wikipedia-r-2.7.50452-r-2023-09-06.zip
Size: 4.42MB
MD5: 5556bafa9a7ffa46dd796aa2edd7b428
SHA1: 245f2f9e672c641a134b9626dc5d699a1e159597
SHA256: 47dcd4a67ff1c788c528899033dd4a15c82f5eb08e5e4868f77384644e6d9656

APP INFORMATION

App Name: @string/app_name_prod
Package Name:
Main Activity:
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 48
Services: 4
Receivers: 4
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: **1** | WARNING: **2** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	org/wikipedia/util/log/L.kt

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	org/wikipedia/createaccount/CreateAccountActivity.kt org/wikipedia/dataclient/mwapi/MwQueryResult.kt org/wikipedia/login/LoginResult.kt org/wikipedia/page/PageActivity.kt org/wikipedia/recurring/TalkOfflineCleanupTask.kt
3	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	org/wikipedia/WikipediaApp.kt
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/wikipedia/gallery/MediaDownloadReceiver.kt org/wikipedia/util/FileUtil.kt org/wikipedia/util/ShareUtil.kt
5	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	org/wikipedia/util/ClipboardUtil.kt
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/wikipedia/dataclient/ServiceFactory.kt

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

EMAILS

EMAIL	FILE
this@editpreviewfragment.model this@editpreviewfragment.linkhandle	org/wikipedia/edit/preview/EditPreviewFragment.kt
this@pagefragment.model this@pagefragment.linkhandle	org/wikipedia/page/PageFragment.kt
this@longpressmenu.entry	org/wikipedia/readinglist/LongPressMenu.kt

HARDCODED SECRETS

POSSIBLE SECRETS
K5IYCQhuLgA6CCUdaSY71m6T7H0TiVaZ8rJ4nSYlUVCqA/viewform
OTdsJ0zpiVW7vfFpWQgZtzQbU0dZEw/viewform
JgxJ8lFRa8UGg4xcWdL6Na18GuDCUD8iUXA/viewform
Rlr8hdpT4oKxYQJD3rdE5RCINl5l6RQ/viewform
c9LERNou7CqhzoSZfL952PKH8bqCGMpA/viewform

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.