



ANDROID STATIC ANALYSIS REPORT



 Diva (1.0)

File Name: DivaApplication.apk

Package Name: jakhar.aseem.diva






Scan Date: Jan. 29, 2024, 10:39 a.m.

App Security Score: **39/100 (HIGH RISK)**

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	7	1	1	1

FILE INFORMATION

File Name: DivaApplication.apk

Size: 1.43MB

MD5: 82ab8b2193b3cfb1c737e3a786be363a

SHA1: 27e849d9d7b86a3a3357fb3e980433a91d416801

SHA256: 5cefc51fce9bd760b92ab2340477f4dda84b4ae0c5d04a8c9493e4fe34fab7c5

APP INFORMATION

App Name: Diva

Package Name: jakhar.aseem.diva

Main Activity: jakhar.aseem.diva.MainActivity

Target SDK: 23

Min SDK: 15

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 17

Services: 0

Receivers: 0

Providers: 1

Exported Activities: 2

Exported Services: 0

Exported Receivers: 0

Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: False

v3 signature: False

v4 signature: False

X.509 Subject: C=US, O=Android, CN=Android Debug

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2015-11-02 08:32:11+00:00

Valid To: 2045-10-25 08:32:11+00:00

Issuer: C=US, O=Android, CN=Android Debug

Serial Number: 0x218330df

Hash Algorithm: sha256

md5: d620162ac34ee974d7fd3a1862e7e4df

sha1: ae4ead5aeaba4e9e4fc928e7c7f7fd459f008031

sha256: 35d7f7ad35dfb826b70fa4b73187ed478540e32c8b8c5653b86568029fcd5840

sha512: e936169585893a7a248e393ddb296b2101432de5b07c3d7e2bdc8070dc0b58277b46e443eff3730b4f5a25b61f78c9078f54cc325cb86c17160b5bae13148d1e

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.



APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	dx (possible dexmerge)
	Manipulator Found	dexmerge



NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 2 | 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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 4 | INFO: 0 | SUPPRESSED: 1

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.
3	Activity (jakhar.aseem.diva.APICredsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (jakhar.aseem.diva.APICreds2Activity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
5	Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 1 | SECURE: 0 | 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	jakhar/aseem/diva/AccessControl1Activity.java jakhar/aseem/diva/AccessControl2Activity.java jakhar/aseem/diva/InsecureDataStorage2Activity.java jakhar/aseem/diva/InsecureDataStorage3Activity.java jakhar/aseem/diva/InsecureDataStorage4Activity.java jakhar/aseem/diva/LogActivity.java jakhar/aseem/diva/SQLInjectionActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	jakhar/aseem/diva/InsecureDataStorage4Activity.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	jakhar/aseem/diva/InsecureDataStorage3Activity.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	jakhar/aseem/diva/InsecureDataStorage2Activity.java jakhar/aseem/diva/NotesProvider.java jakhar/aseem/diva/SQLInjectionActivity.java
5	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	jakhar/aseem/diva/BuildConfig.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	--------------	-------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libdivajni.so	<p>False</p> <p>high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>True</p> <p>info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO</p> <p>info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None</p> <p>info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None</p> <p>info</p> <p>The binary does not have RUNPATH set.</p>	<p>False</p> <p>warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False</p> <p>warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	mips/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	mips64/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86/libdivajni.so	<p>False</p> <p>high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>True</p> <p>info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO</p> <p>info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None</p> <p>info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None</p> <p>info</p> <p>The binary does not have RUNPATH set.</p>	<p>False</p> <p>warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False</p> <p>warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	mips/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	mips64/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	x86_64/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libdivajni.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NIAP ANALYSIS v1.3

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

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/24	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET
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.

OFAC SANCTIONED COUNTRIES

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

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
payatu.com	ok	IP: 104.21.39.160 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"pkey" : "notespin"

Report Generated by - MobSF v3.9.3 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.