com.apksonar.demo.nativedeep

demo-nativedeep-aligned-debugSigned.apk · SHA-256 c79afac775b1f5cd… · deep scan · finished 2026-11-18T19:59:54 UTC

HIGH × 10 | MEDIUM × 10 | INFO × 3 | 83 secret families | OWASP MASVS | CVSS 3.1

OWASP MASVS: RESILIENCE · NETWORK · PLATFORM · CODE · CRYPTO

APPLICATION

version 1.0 (1) · SDK 24→35 · 404.6 KB · 9 files · 1 dex

FINDINGS · 23

Anti-debugging via ptrace in native code

lib/x86_64/libapksonar_native.so

ptrace@GLIBC_2.2.5

The native library calls ptrace (typically PTRACE_TRACEME self-attach) so the app aborts under a debugger — a classic anti-analysis technique that hides behavior from dynamic inspection

native · MASVS-RESILIENCE · CVSS 5.9

Custom TLS verification hook in native code

lib/x86_64/libapksonar_native.so

SSL_CTX_set_verify

The library can override OpenSSL certificate verification (SSL_CTX_set_verify) — often used to accept self-signed MITM certificates

native · MASVS-RESILIENCE · CVSS 5.9

Executes external programs from native code

lib/x86_64/libapksonar_native.so

execve@GLIBC_2.2.5

The library spawns other binaries (execve) — can drop and run payloads invisible to Java-layer analysis

native · MASVS-RESILIENCE · CVSS 5.9

Frida anti-hooking detection in native code

lib/x86_64/libapksonar_native.so

frida

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 5.9

Debugger detection via /proc TracerPid in native code

lib/x86_64/libapksonar_native.so

TracerPid

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 5.9

High-entropy native library (packed or encrypted)

lib/x86_64/libsec_payload.so

entropy 8.00 (threshold 7.2)

The library's byte entropy approaches that of compressed/encrypted data. Packers hide code from static analysis and are common in malware and DRM.

native · MASVS-RESILIENCE · CVSS 5.9

TrustManager.checkServerTrusted is empty — certificate validation disabled

com.apksonar.demo.nativedeep.TrustAllCerts

checkServerTrusted() { }

A custom X509TrustManager accepts every certificate without checks. Combined with an HTTPS client this disables protection against MITM.

tls · MASVS-NETWORK · CVSS 6.8

TrustManager.checkClientTrusted is empty — certificate validation disabled

com.apksonar.demo.nativedeep.TrustAllCerts

checkClientTrusted() { }

A custom X509TrustManager accepts every certificate without checks. Combined with an HTTPS client this disables protection against MITM.

tls · MASVS-NETWORK · CVSS 6.8

HostnameVerifier always returns true

com.apksonar.demo.nativedeep.LenientHostname

```
return true;
```

Hostname verification is disabled: any certificate is accepted for any host — the classic companion of a trust-all TrustManager in MITM-vulnerable apps.

tls · MASVS-NETWORK · CVSS 6.8

JavaScript bridge exposed to web content (addJavascriptInterface)

com.apksonar.demo.nativedeep.MainActivity

```
addJavascriptInterface(...)
```

The WebView registers a Java object callable from JavaScript. If the page or an XSS in it is attacker-controlled, the bridge methods run with the app's full permissions.

webview · MASVS-PLATFORM · CVSS 6.8

Direct certificate verification call in native code

lib/x86_64/libapksonar_native.so

```
X509_verify_cert
```

Manual X.509 chain verification code — legitimate in some apps, but also the usual hook point for certificate pinning bypasses

native · MASVS-RESILIENCE · CVSS 3.7

Raw syscall interface used in native code

lib/x86_64/libapksonar_native.so

```
syscall@GLIBC_2.2.5
```

Direct syscalls bypass libc hooks used by security tooling — common in packers and hidden-behavior payloads

native · MASVS-RESILIENCE · CVSS 3.7

Xposed framework detection in native code

lib/x86_64/libapksonar_native.so

```
xposed
```

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 3.7

Magisk root detection in native code

lib/x86_64/libapksonar_native.so

```
magisk
```

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 3.7

su binary probing in native code

lib/x86_64/libapksonar_native.so

```
/system/bin/su
```

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 3.7

Reads own process status (debugger self-check)

lib/x86_64/libapksonar_native.so

```
/proc/self/status
```

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 3.7

Reads own memory maps (hook/framework detection)

lib/x86_64/libapksonar_native.so

```
/proc/self/maps
```

Ghidra string analysis of the native library

native · MASVS-RESILIENCE · CVSS 3.7

Signed with a debug certificate

```
C=US
ST=US
L=US
O=US
OU=Android
CN=Android Debug
```

The APK is signed with the Android Debug certificate. Debug builds must never ship: they can be trivially replaced and usually enable extra logging and debugging paths.

signing · MASVS-CODE · CVSS 4.8

Packed native library: libsec_payload.so

libsec_payload.so

UPX packer marker

The .so is packed with UPX. Packing hides the real code from static analysis and is common in obfuscated SDKs, cheats and malware loaders.

native · MASVS-RESILIENCE · CVSS 3.7

Outdated OpenSSL 1.0.2u statically linked in libsec_payload.so

libsec_payload.so

OpenSSL 1.0.2u

OpenSSL 1.0.x/1.1.x is EOL and carries known CVEs; it is compiled into the app, so updates depend on the app vendor, not the OS.

crypto · MASVS-CRYPTO · CVSS 7.4

Forks child processes

lib/x86_64/libapksonar_native.so

fork@GLIBC_2.2.5

Forking from native code is used by watchdogs, packers and background workers alike

native · MASVS-RESILIENCE

Runtime library loading (dlopen)

lib/x86_64/libapksonar_native.so

dlopen@GLIBC_2.34

The library loads other .so files at runtime — code that static Java-level review cannot see

native · MASVS-RESILIENCE

Runtime symbol resolution (dlsym)

lib/x86_64/libapksonar_native.so

dlsym@GLIBC_2.34

Symbols are resolved at runtime — frequently used to hide calls behind generic handles

native · MASVS-RESILIENCE

PERMISSIONS · 2 (1 dangerous)

INTERNET READ_PHONE_STATE

COMPONENTS · 1 activities · 0 services · 0 receivers · 0 providers · 1 exported

MainActivity

NATIVE LIBRARIES · 2

libapksonar_native.so · x86_64 · 16.2 KB
libsec_payload.so · x86_64 · 390.8 KB · 1.0.2u · packer: UPX

NATIVE ANALYSIS · GHIDRA · 2 libs

libapksonar_native.so · x86_64 · 56 procedures · 104 strings · 16.2 KB · entropy 2.38 · shared

ptrace@GLIBC_2.2.5 (anti-debug) SSL_CTX_set_verify (tls-bypass) X509_verify_cert (tls-bypass)
syscall@GLIBC_2.2.5 (raw-syscall) execve@GLIBC_2.2.5 (shell-exec) fork@GLIBC_2.2.5 (process-spawn)
dlopen@GLIBC_2.34 (dynamic-loading) dlsym@GLIBC_2.34 (dynamic-loading)
frida (anti-analysis) xposed (anti-analysis) magisk (root-detection) /system/bin/su (root-detection)
/system/xbin/su (root-detection) TracerPid (anti-debug) /proc/self/status (anti-debug)
/proc/self/maps (anti-analysis)
Java_com_apksonar_demo_nativedeep_NativeBridge_insecureTls
Java_com_apksonar_demo_nativedeep_NativeBridge_getToken
Java_com_apksonar_demo_nativedeep_NativeBridge_spawnWatchdog
Java_com_apksonar_demo_nativedeep_NativeBridge_init
Java_com_apksonar_demo_nativedeep_NativeBridge_isDeviceRooted JNI_OnLoad

Ghidra decompiler · JNI_OnLoad

```
undefined8 JNI_OnLoad(void)

{
ptrace(PTRACE_TRACEME,0,0,0);
return 0x10006;
}
```

libsec_payload.so · x86_64 · 0 procedures · 0 strings · 390.8 KB · entropy 8 · shared

JAVA ANALYSIS · JADX · 6 classes · obfuscation 0%

com.apksonar.demo.nativedeep (6)

⚠ empty: com.apksonar.demo.nativedeep.TrustAllCerts.checkServerTrusted()
⚠ empty: com.apksonar.demo.nativedeep.TrustAllCerts.checkClientTrusted()
⚠ always-true: com.apksonar.demo.nativedeep.LenientHostname.verify()
⚠ WebView com.apksonar.demo.nativedeep.MainActivity: addJavascriptInterface
⚠ WebView com.apksonar.demo.nativedeep.MainActivity: setJavaScriptEnabled(true)

SIGNATURE

scheme: v3 · C=US
ST=US
L=US
O=US
OU=Android
CN=Android Debug · rsa
valid 2016-10-23 → 2044-03-10 · cert SHA-256 1e08a903aef9c3a7…