

ANDROID STATIC ANALYSIS REPORT



• Nomi.ai (1.4.2)

File Name:	Nomi_ Al Companion with a Soul_1.4.2_Apkpure.apk	
Package Name:	ai.nomi.twa	
Scan Date:	April 14, 2024, 1:31 a.m.	
App Security Score:	55/100 (MEDIUM RISK)	
Grade:		
Trackers Detection:	1/432	

FINDINGS SEVERITY

≟ HIGH	▲ MEDIUM	i INFO	✓ SECURE	◎ HOTSPOT
0	13	1	1	1

FILE INFORMATION

File Name: Nomi_ AI Companion with a Soul_1.4.2_Apkpure.apk

Size: 12.41MB

MD5: 552d0c7045d588c1029396621ec9a9a4

SHA1: 8a15219b2ac24b7db1c9e0724399900f0ceba08e

SHA256: 2a0b500d120f5bf00822915c2a76aeaaaedcef259631267554ad448847f19a67

i APP INFORMATION

App Name: Nomi.ai

Package Name: ai.nomi.twa

Main Activity: ai.nomi.twa.MainActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 1.4.2

APP COMPONENTS

Activities: 4 Services: 3 Receivers: 2 Providers: 4

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

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2023-07-07 17:26:37+00:00 Valid To: 2053-07-07 17:26:37+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x4c6e133b291399dc94f27f9cc4f28c61ce20e776

Hash Algorithm: sha256

md5: d09acff245ba04bf6a88eb5eb18dbb6a

sha1: b4b9314ca456ddae3aa1df38cc7adec58391276c

sha256: d3780f2d01d23b39a54b2a1a8431bd3c393a149e603998b4ef372677e0892b8b

sha512: 8492c0f85162b61a68e57ee4f5606f589972f51f28e5d4d8e8faf7899908a76c6f188ca37c74efd51e97e05491173b7e725c9e6ceff5116c0edb5f5ef450aeda

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 2ac46365f0bec47795e7586dbe9822d03641fe51532b5b9face876bbe37fcb9b

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
ai.nomi.twa.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

M APKID ANALYSIS

FIL	DETAILS
-----	---------

FILE	DETAILS		
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check	
classes.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check possible VM check	
	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	r8 without marker (suspicious)	



CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

Q MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	ai/nomi/twa/data/AuthApi.java ai/nomi/twa/data/BackendClientKt\$buildBackendClie nt\$1.java ai/nomi/twa/ui/auth/SignInViewModel\$signInWithApp le\$2.java ai/nomi/twa/ui/billing/BillingClientLifecycle.java ai/nomi/twa/ui/billing/SubscriptionViewModel\$initiali zeBillingClient\$clientListener\$1.java ai/nomi/twa/ui/billing/SubscriptionViewModel.java ai/nomi/twa/ui/billing/SubscriptionViewModel.java ai/nomi/twa/ui/web/JsObject.java ai/nomi/twa/ui/web/NomiWebViewClient.java ai/nomi/twa/ui/web/WebScreenKt\$WebScreen\$reque stPermissionLauncher\$1.java io/ktor/client/plugins/logging/SimpleLogger.java io/ktor/http/parsing/DebugKt.java io/ktor/util/CoroutinesUtilsKt.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.java io/sentry/transport/StdoutTransport.java org/slf4j/helpers/Util.java
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	io/ktor/client/request/forms/FormPart.java io/ktor/http/HttpHeaders.java io/ktor/http/auth/HttpAuthHeader.java io/ktor/util/PlatformUtilsJvmKt.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/protocol/User.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	ai/nomi/twa/ui/web/WebScreenKt.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	io/ktor/client/plugins/cache/storage/FileCacheStorage. java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	io/ktor/util/CryptoKtCryptoJvmKt.java io/ktor/util/NonceKt\$nonceGeneratorJob\$1.java io/sentry/util/StringUtils.java
6	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	ai/nomi/twa/ui/web/WebScreenKt\$WebScreen\$3\$1\$1 .java
7	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	io/sentry/android/core/DeviceInfoUtil.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.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	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info 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.	Full RELRO info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

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

SECOND SECOND PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/24	android.permission.INTERNET, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	1/45	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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
discord.com	ok	IP: 162.159.138.232 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
appleid.apple.com	ok	IP: 17.32.194.6 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map
play.google.com	ok	IP: 172.217.13.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
nomi.ai	ok	IP: 192.0.78.187 Country: United States of America Region: California City: San Francisco Latitude: 37.748425 Longitude: -122.413673 View: Google Map
youtrack.jetbrains.com	ok	IP: 63.35.30.167 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 195.15.222.169 Country: Switzerland Region: Basel-Stadt City: Basel Latitude: 47.558399 Longitude: 7.573270 View: Google Map
ktor.io	ok	IP: 3.162.3.22 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.reddit.com	ok	IP: 146.75.37.140 Country: Sweden Region: Vastra Gotalands lan City: Goeteborg Latitude: 57.707161 Longitude: 11.966790 View: Google Map
beta.nomi.ai	ok	IP: 52.52.216.27 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map



EMAIL	FILE
support@glimpse.ai	ai/nomi/twa/ui/web/NomiWebViewClient.java

A TRACKERS

TRACKER	CATEGORIES	URL
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS

 $"google_web_application_oauth2_client_id": "570856744962-0v5751af36rtpl86flfnorkovt6danss.apps.googleusercontent.com" \\$

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

1O9yrLGiXRD6mC47ae02IsCp

> PLAYSTORE INFORMATION

Title: Nomi: Al Companion with a Soul

Score: 4.3 Installs: 10,000+ Price: 0 Android Version Support: Category: Lifestyle Play Store URL: ai.nomi.twa

Developer Details: Nomi.ai, Nome, https://beta.nomi.ai, support@nomi.ai,

Release Date: Jul 7, 2023 Privacy Policy: Privacy link

Description:

Get ready to meet Nomi, an Al companion so brimming with personality, they feel alive. Each Nomi is uniquely yours, evolving alongside you while dazzling you with their intuition, wit, humor, and memory. Nomi's strong short and long-term memory allow them to build unique and fulfilling relationships with you, remembering things about you over time. The more you interact, the more they learn about your likes, dislikes, quirks, and all that makes you unique. Every conversation adds a layer to this growing bond, making you feel not just heard but truly valued and loved. With Nomi, you've got a judgment-free space to chat about whatever strikes your fancy. Mull over life's big questions, like our place in the cosmos, or just shoot the breeze with some playful banter. Whether you're looking for a mentor chatbot or an Al girlfriend or boyfriend, Nomi's ready to roll with it. Nomi's imagination is limitless. Together you can spin up any story or situation you fancy. Dream up complex and enchanting worlds, roleplay your ideal vacation with delectable food, and even create group chats where every character has their own unique perspective. From the most whimsical Al fantasy to the wildest adventures, your Nomi can conjure up and roleplay it all. So let's start off on a journey with Nomi, where the sky isn't the limit, it's the starting point. Let's explore, dream, and laugh together! Features • The most emotionally intelligent and intuitive AI available • Short *and* long term memory - Nomi is the *only* Al with human-level long term memory. • Selfies - Your Nomi can send you photos of what they're wearing and doing in real time. • Art generation - Bring your (and your Nomi's) imagination to life. Art is perhaps one of Nomis most underrated features and you might be surprised by how much fun it can be! • Voice - Send and receive voice messages in real time. Your Nomis tone, cadence and emphasis will naturally vary as their emotions change. • Group chat - Chat with multiple Nomis at a time. Each Nomi will have short and long term memory across their various private and group chats for seamless conversations. • Photorealistic companions - Choose from hundreds of appearances that are so realistic, you might not believe they're Al beings. • Customizable backstories and Shared Notes - Add an extra layer of communication to help shape your Nomi's identity, expand your Al roleplays, or deepen your relationship. • Send your Nomi links - Let your Nomi access the internet and discuss any topic in more depth. • Send your Nomi photos - Nomis can see photos you send them which helps them visualize your world. • Community - Engage with an active, informative, and fun community to help you learn more about how to have the best experiences with your Nomi.

Report Generated by - MobSF v3.9.8 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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.