ANDROID STATIC ANALYSIS REPORT

SALTO Nebula (0.14.1)

File Name:	Salto_Nebula.apk

Package Name:	com.saltosystems.android.nebula
Scan Date:	Jan. 3, 2026, 6:28 a.m.
App Security Score:	61/100 (LOW RISK)
Grade:	A
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	15	2	4	1

FILE INFORMATION

File Name: Salto_Nebula.apk
Size: 45.35MB
MD5: a65ef0c6310d07a73a8c54f758a6fd03
SHA1: abccc2fa257eaa2f35eb1283cbfc9f7e6880c186
SHA256: 339da96fcca32501da4fbec7c9d9e7075c42136f49b95e383b614ce00ef8a9f6

APP INFORMATION

App Name: SALTO Nebula
Package Name: com.saltosystems.android.nebula
Main Activity: com.saltosystems.android.nebula.ui.MainActivity
Target SDK: 33
Min SDK: 24
Max SDK:
Android Version Name: 0.14.1
Android Version Code: 1401900

APP COMPONENTS

Activities: 5

Services: 11
Receivers: 12
Providers: 2
Exported Activities: 2
Exported Services: 2
Exported Receivers: 2
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: 2021-05-14 11:18:14+00:00
Valid To: 2051-05-14 11:18:14+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xd3935031418c586686bc523f0b1bd8b2eb2db17a
Hash Algorithm: sha256
md5: 3b163e0ba13d5eae448cc03fc2733a6b
sha1: fb3fdb4008f32e5d8f48d0fbad0ce9abf80bb74f
sha256: 4b467b79ef7e5db7738f6e0b1d70d7678dc20826f0203986e97cabac4d60f05d
sha512: 947b2e93c9ac0e522da6a627583a455eddf5c16c9997589471519a0cf59222f2031eaa46d6b383b2337120188d291e843ddd461a08dfe63df848001a0b802ef8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 01a802865def90eaa61a7e57d4aa11a8cd2e5402bbf09b516e206fda1158ccc4
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.saltosystems.android.nebula.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>lib/arm64-v8a/libtoolChecker.so</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>anti_root</td><td>RootBeer</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libtoolChecker.so</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>anti_root</td><td>RootBeer</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>lib/x86/libtoolChecker.so</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>anti_root</td><td>RootBeer</td></tr></table></td></tr>
<tr><td>lib/x86_64/libtoolChecker.so</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>anti_root</td><td>RootBeer</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.saltosystems.android.nebula.ui.MainActivity	Schemes: https://, Hosts: nebula.saltosystems.com, dev.nebula.saltosystems.com, Paths: /,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: https://, Hosts: nebula.saltosystems.com, dev.nebula.saltosystems.com, Paths: /oauth2redirect,

NETWORK SECURITY

HIGH: **0** | WARNING: **1** | INFO: **0** | SECURE: **1**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.
2	nebula.saltoapis.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	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.
4	Service (com.saltosystems.android.nebula.shared.domain.digitalkey.hce.NebulaHceService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_SERVICE [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.
5	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	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.
6	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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.
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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: **6** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/recovery/ResilientOutputStreamBase.java ch/qos/logback/core/spi/ContextAwareBase.java ch/qos/logback/core/spi/ContextAwareImpl.java com/saltosystems/android/nebula/obscured/AbstractC0921Je0.java com/saltosystems/android/nebula/obscured/A

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bstractC1230Qg0.java com/saltosystems/android/nebula/obscured/AbstractC1896c8.java com/saltosystems/android/nebula/obscured/AbstractC2201en0.java com/saltosystems/android/nebula/obscured/AbstractC2293fb0.java com/saltosystems/android/nebula/obscured/AbstractC2396gK0.java com/saltosystems/android/nebula/obscured/AbstractC2514hL0.java com/saltosystems/android/nebula/obscured/AbstractC2561hn0.java com/saltosystems/android/nebula/obscured/AbstractC2742jK0.java com/saltosystems/android/nebula/obscured/AbstractC2793jo0.java com/saltosystems/android/nebula/obscured/AbstractC2937l2.java com/saltosystems/android/nebula/obscured/AbstractC2947l7.java com/saltosystems/android/nebula/obscured/AbstractC3406p40.java com/saltosystems/android/nebula/obscured/AbstractC3825si.java com/saltosystems/android/nebula/obscured/AbstractC3896tH.java com/saltosystems/android/nebula/obscured/AbstractC3905tL0.java com/saltosystems/android/nebula/obscured/AbstractC4241wE0.java com/saltosystems/android/nebula/obscured/AbstractC4593zE0.java com/saltosystems/android/nebula/obscured/BD0.java com/saltosystems/android/nebula/obscured/BI0.java com/saltosystems/android/nebula/obscured/C1157On.java com/saltosystems/android/nebula/obscured/C1496Wn.java com/saltosystems/android/nebula/obscured/C1739an0.java com/saltosystems/android/nebula/obscured/C

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	1743ap0.java com/saltosystems/android/nebula/obscured/C1914cH.java com/saltosystems/android/nebula/obscured/C2114e10.java com/saltosystems/android/nebula/obscured/C2192ej.java com/saltosystems/android/nebula/obscured/C2284fU.java com/saltosystems/android/nebula/obscured/C2383gE.java com/saltosystems/android/nebula/obscured/C2692iw.java com/saltosystems/android/nebula/obscured/C2698iz.java com/saltosystems/android/nebula/obscured/C2746jM0.java com/saltosystems/android/nebula/obscured/C2849kG.java com/saltosystems/android/nebula/obscured/C2858kK0.java com/saltosystems/android/nebula/obscured/C3340oW.java com/saltosystems/android/nebula/obscured/C3405p4.java com/saltosystems/android/nebula/obscured/C3775sE0.java com/saltosystems/android/nebula/obscured/C3860sz0.java com/saltosystems/android/nebula/obscured/C4065ul.java com/saltosystems/android/nebula/obscured/C4363xF0.java com/saltosystems/android/nebula/obscured/C4475yD0.java com/saltosystems/android/nebula/obscured/C4533yl.java com/saltosystems/android/nebula/obscured/C4566z1.java com/saltosystems/android/nebula/obscured/GX.java com/saltosystems/android/nebula/obscured/HX.java com/saltosystems/android/nebula/obscured/InputConnectionC2439gk0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				putConnectionC2459gk0.java com/saltosystems/android/nebula/obscured/InterfaceC4210vz0.java com/saltosystems/android/nebula/obscured/JW.java com/saltosystems/android/nebula/obscured/JX.java com/saltosystems/android/nebula/obscured/Jz0.java com/saltosystems/android/nebula/obscured/K7.java com/saltosystems/android/nebula/obscured/L20.java com/saltosystems/android/nebula/obscured/LA0.java com/saltosystems/android/nebula/obscured/LayoutInflaterFactory2C3063m7.java com/saltosystems/android/nebula/obscured/M20.java com/saltosystems/android/nebula/obscured/M8.java com/saltosystems/android/nebula/obscured/ML.java com/saltosystems/android/nebula/obscured/MenuItemC1768b10.java com/saltosystems/android/nebula/obscured/O7.java com/saltosystems/android/nebula/obscured/OK0.java com/saltosystems/android/nebula/obscured/Q9.java com/saltosystems/android/nebula/obscured/RG0.java com/saltosystems/android/nebula/obscured/S7.java com/saltosystems/android/nebula/obscured/SG0.java com/saltosystems/android/nebula/obscured/TG0.java com/saltosystems/android/nebula/obscured/ViewOnClickListenerC3047lz0.java com/saltosystems/android/nebula/obscured/ViewOnLongClickListenerC3659rE0.java com/saltosystems/android/nebula/obscured/W1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/saltosystems/android/nebula/obscured/W30.java com/saltosystems/android/nebula/obscured/W7.java com/saltosystems/android/nebula/obscured/XG0.java com/saltosystems/android/nebula/obscured/Y00.java com/saltosystems/android/nebula/obscured/Y1.java com/saltosystems/srpc/io/SrpcLog.java net/openid/appauth/internal/Logger.java org/slf4j/helpers/Util.java
2	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	com/saltosystems/android/nebula/obscured/C1743ap0.java com/saltosystems/android/nebula/obscured/M20.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java com/saltosystems/android/nebula/obscured/AbstractC1796bF0.java com/saltosystems/android/nebula/obscured/C1039Lz.java com/saltosystems/android/nebula/obscured/C1668aE0.java com/saltosystems/android/nebula/obscured/C1684aM0.java com/saltosystems/android/nebula/obscured/C3202nI0.java com/saltosystems/android/nebula/obscured/M00.java com/saltosystems/android/nebula/obscured/Qu0.java net/openid/appauth/ClientSecretPost.java net/openid/appauth/RegistrationResponse.java net/openid/appauth/TokenRequest.java
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	ch/qos/logback/core/android/AndroidContextUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java com/saltosystems/android/nebula/obscured/C1514Xb.java com/saltosystems/android/nebula/obscured/C2902kl.java com/saltosystems/android/nebula/obscured/C3583qc0.java com/saltosystems/android/nebula/obscured/P80.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/saltosystems/android/nebula/obscured/AbstractC3630r0.java com/saltosystems/android/nebula/obscured/AbstractC4302wn0.java com/saltosystems/android/nebula/obscured/C0554Ao0.java com/saltosystems/android/nebula/obscured/C0906Iu.java com/saltosystems/android/nebula/obscured/C1301Rz.java com/saltosystems/android/nebula/obscured/C1307Sc0.java com/saltosystems/android/nebula/obscured/C1557Yb0.java com/saltosystems/android/nebula/obscured/C1707ac0.java com/saltosystems/android/nebula/obscured/C3015lj0.java com/saltosystems/android/nebula/obscured/C3068m90.java com/saltosystems/android/nebula/obscured/C3859sz.java com/saltosystems/android/nebula/obscured/SL0.java com/saltosystems/android/nebula/obscured/T70.java com/saltosystems/android/nebula/obscured/V70.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	ch/qos/logback/classic/android/SQLiteAppender.java com/saltosystems/android/nebula/obscured/C3425pE.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/saltosystems/android/nebula/obscured/AbstractC3134ml.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/saltosystems/android/nebula/obscured/C3257no0.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64/libsrpc_android_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__FD_SET_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ch/qos/logback/core/joran/GenericConfigurator.java ch/qos/logback/core/joran/action/PropertyAction.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/saltosystems/android/nebula/obscured/AbstractC1580Yn.java com/saltosystems/android/nebula/obscured/AbstractC1896c8.java com/saltosystems/android/nebula/obscured/AbstractC2372g80.java com/saltosystems/android/nebula/obscured/C1340Sw.java com/saltosystems/android/nebula/obscured/C1743ap0.java com/saltosystems/android/nebula/obscured/C2698iz.java com/saltosystems/android/nebula/obscured/RG0.java com/saltosystems/android/nebula/obscured/XG0.java
00022	Open a file from given absolute path of the file	file	ch/qos/logback/classic/android/SQLiteAppender.java ch/qos/logback/core/FileAppender.java ch/qos/logback/core/android/AndroidContextUtil.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/FileFinder.java ch/qos/logback/core/rolling/helper/RenameUtil.java com/saltosystems/android/nebula/obscured/C0886Ii0.java com/saltosystems/android/nebula/obscured/C1155Om.java com/saltosystems/android/nebula/obscured/C1743ap0.java com/saltosystems/android/nebula/obscured/C3543qE.java com/saltosystems/android/nebula/obscured/InterfaceC2098du.java com/saltosystems/android/nebula/obscured/M20.java io/realm/e.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java
00012	Read data and put it into a buffer stream	file	ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/saltosystems/android/nebula/obscured/C2698iz.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/saltosystems/android/nebula/obscured/W1.java com/saltosystems/android/nebula/shared/auth/AuthConfiguration.java com/saltosystems/android/nebula/ui/digitalkey/DigitalKeyListFragment.java com/saltosystems/android/nebula/ui/menu/MenuFragment.java com/saltosystems/android/nebula/ui/profile/ProfileLegalFragment.java net/openid/appauth/AuthorizationException.java
00189	Get the content of a SMS message	sms	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00188	Get the address of a SMS message	sms	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00200	Query data from the contact list	collection contact	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00187	Query a URI and check the result	collection sms calllog calendar	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00201	Query data from the call log	collection calllog	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/saltosystems/android/nebula/obscured/AbstractC4588zC.java
00162	Create InetSocketAddress object and connecting to it	socket	com/saltosystems/android/nebula/obscured/C3583qc0.java com/saltosystems/android/nebula/obscured/I4.java
00163	Create new Socket and connecting to it	socket	com/saltosystems/android/nebula/obscured/C3583qc0.java com/saltosystems/android/nebula/obscured/I4.java
00202	Make a phone call	control	com/saltosystems/android/nebula/ui/digitalkey/DigitalKeyListFragment.java
00203	Put a phone number into an intent	control	com/saltosystems/android/nebula/ui/digitalkey/DigitalKeyListFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/saltosystems/android/nebula/obscured/W1.java com/saltosystems/android/nebula/shared/auth/AuthConfiguration.java com/saltosystems/android/nebula/ui/digitalkey/DigitalKeyListFragment.java
00026	Method reflection	reflection	com/saltosystems/android/nebula/obscured/WN.java com/saltosystems/android/nebula/obscured/XN.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/saltosystems/android/nebula/obscured/C1621Zm0.java com/saltosystems/android/nebula/obscured/ViewOnClickListenerC3047lz0.java com/saltosystems/android/nebula/obscured/W1.java com/saltosystems/android/nebula/shared/auth/AuthConfiguration.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	com/saltosystems/android/nebula/obscured/C4566z1.java
00091	Retrieve data from broadcast	collection	net/openid/appauth/AuthorizationManagementActivity.java
00114	Create a secure socket connection to the proxy address	network command	com/saltosystems/android/nebula/obscured/C1487Wi0.java
00079	Hide the current app's icon	evasion	com/saltosystems/android/nebula/obscured/S90.java
00191	Get messages in the SMS inbox	sms	com/saltosystems/android/nebula/obscured/ViewOnClickListenerC3047lz0.java
00147	Get the time of current location	collection location	com/saltosystems/android/nebula/obscured/C4363xF0.java
00075	Get location of the device	collection location	com/saltosystems/android/nebula/obscured/C4363xF0.java
00115	Get last known location of the device	collection location	com/saltosystems/android/nebula/obscured/C4363xF0.java
00039	Start a web server	control network	ch/qos/logback/classic/net/SimpleSocketServer.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/AuthorizationServiceConfiguration.java
00096	Connect to a URL and set request method	command network	net/openid/appauth/AuthorizationService.java
00089	Connect to a URL and receive input stream from the server	command network	net/openid/appauth/AuthorizationService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	net/openid/appauth/AuthorizationService.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nebula-5dd63.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/751987927667/namespaces/firebase:fetch?key=AIzaSyDs8heuIYz-AZWVJufuqwm6Airo9yheb-k. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	4/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

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
saltosystems.com	ok	**IP:** 151.101.2.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 192.178.50.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
nebula-5dd63.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
logback.qos.ch	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
docs.mongodb.com	ok	**IP:** 3.33.186.135 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.saltosystems.com	ok	**IP:** 151.101.66.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"device_configuration_gateway_wifi_password" : "Passwort"
"device_configuration_gateway_wifi_password" : "Heslo"
"device_configuration_gateway_wifi_password" : "Wachtwoord"
"device_configuration_gateway_wifi_password" : "Passord"

POSSIBLE SECRETS
"device_configuration_gateway_wifi_password" : "Contraseña"
"google_api_key" : "AIzaSyDs8heuIYz-AZWVJufuqwm6Airo9yheb-k"
"device_configuration_gateway_wifi_password" : "Hasło"
"firebase_database_url" : "https://nebula-5dd63.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyDs8heuIYz-AZWVJufuqwm6Airo9yheb-k"
"com.google.firebase.crashlytics.mapping_file_id" : "8743f0dd3316441c90a006c5a844c5c5"
"device_configuration_gateway_wifi_password" : "□□□□"
"device_configuration_gateway_wifi_password" : "Password"
58EE46A1DF1DBD48AB14301D0603551D250416301406082B0601050507030206082B06010505070301301D060355
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
BA1830F9DA0FD1333FC595AE9E
470fa2b4ae81cd56ecbcda9735803434cec591fa
B6E60002-E2E3-BC82-4C72-929D0D29CA17
B6E60003-E2E3-BC82-4C72-929D0D29CA17
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
04030C1B53414C544F2053595354454D53204445564943455320434120473131193017060355040A0C1053414C54

POSSIBLE SECRETS
c103703e120ae8cc73c9248622f3cd1e
B6E60001-E2E3-BC82-4C72-929D0D29CA17
0A0C1053414C544F2053595354454D5320534C3111300F06035504070C084F696172747A756E310B300906035504
30818330120603551D130101FF040830060101FF020100301F0603551D23041830168014C8DC7F7AEB08997DDF53
3082028D308201EEA003020102021461BEC7B3A17A426098805B872802BCC1124F6CDA300A06082A8648CE3D0403
115792089210356248762697446949407573530086143415290314195533631308867097853951
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
7fmduHKTdHHrlMvldlEqAIlSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1QIw
02305E3121301F06035504030C1853414C544F2053595354454D5320524F4F5420434120473131193017060355040
2A8648CE3D04030203818C00308188024201C905410F1457E088C0B70CF2B5A37FB46F2F3D76C7220C2022B4C7C4
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
115792089210356248762697446949407573529996955224135760342422259061068512044369
49f946663a8deb7054212b8adda248c6

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
F2D8BD730CB0D11075873FE5ACD05F4BA7B420888CC41C1A5D09C55C84C16BD044E1D48313618ABBE0F7DAA38186
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
ED3B20EBAAF635ED6E9B9D430EB6699EB269148E231C74B2385762EF744C47930A6B36C7620242019A15D6468CBB
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
301306072A8648CE3D020106082A8648CE3D030107034200004D4BC3FBCE31ACE08D229CD0D7D1554C407763E9CA1
4F2053595354454D5320534C3111300F06035504070C084F696172747A756E310B30090603550406130245533059
29E56147AA13BB9310E782B0B60FC44CF7BBF52CF58E5EA1CA5BB1AD05E1D6126FB55EA87876396A22B5866E0D58
1D0E04160414FEEC6D991B9D9CE62C42911D532B5A078C6AE448300E0603551D0F0101FF040403020106300A0608
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

PLAYSTORE INFORMATION

Title: Salto Nebula

Score: None **Installs:** 1,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** com.saltosystems.android.nebula

Developer Details: Salto Systems S.L., Salto+Systems+S.L., None, https://www.saltosystems.com, android@saltosystems.com,

Release Date: Nov 10, 2022 **Privacy Policy:** Privacy link

Description:

The Salto Nebula app allows you to use your phone as a key and is part of Salto's cloud-based Nebula access control platform. You can also use the app to configure Salto devices like electronic locks. About Salto Systems: Salto Systems revolutionized access control with the introduction of the Salto Virtual Network SVN data-on-card technology and the advanced battery-operated wireless electronic smart door lock range in 2001. For over 20 years Salto has been synonymous with innovative solutions, including stand-alone, cloud-based and mobile applications, that set new standards in security, manageability, flexibility and design that bring real-world benefits to virtually any door and building type. Across a broad range of industries and applications, Salto is widely recognized as a global market leader in smart electronic access control solutions.

SCAN LOGS

Timestamp	Event	Error
2026-01-03 06:28:45	Generating Hashes	OK
2026-01-03 06:28:45	Extracting APK	OK
2026-01-03 06:28:45	Unzipping	OK
2026-01-03 06:28:45	Parsing APK with androguard	OK
2026-01-03 06:28:45	Extracting APK features using aapt/aapt2	OK

2026-01-03 06:28:45	Getting Hardcoded Certificates/Keystores	OK
2026-01-03 06:28:46	Parsing AndroidManifest.xml	OK
2026-01-03 06:28:46	Extracting Manifest Data	OK
2026-01-03 06:28:46	Manifest Analysis Started	OK
2026-01-03 06:28:46	Reading Network Security config from network_security_config.xml	OK
2026-01-03 06:28:46	Parsing Network Security config	OK
2026-01-03 06:28:46	Performing Static Analysis on: SALTO Nebula (com.saltosystems.android.nebula)	OK
2026-01-03 06:28:46	Fetching Details from Play Store: com.saltosystems.android.nebula	OK
2026-01-03 06:28:47	Checking for Malware Permissions	OK
2026-01-03 06:28:47	Fetching icon path	OK
2026-01-03 06:28:47	Library Binary Analysis Started	OK
2026-01-03 06:28:47	Analyzing lib/armeabi-v7a/libtoolChecker.so	OK

2026-01-03 06:28:47	Analyzing lib/armeabi-v7a/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing lib/armeabi-v7a/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing lib/x86/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing lib/x86/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing lib/x86/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing lib/arm64-v8a/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing lib/arm64-v8a/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing lib/arm64-v8a/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing lib/x86_64/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing lib/x86_64/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing lib/x86_64/librealm-jni.so	OK

2026-01-03 06:28:47	Analyzing apktool_out/lib/armeabi-v7a/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/armeabi-v7a/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/x86/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/x86/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/x86/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/arm64-v8a/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/arm64-v8a/libsrpc_android_jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/arm64-v8a/librealm-jni.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/x86_64/libtoolChecker.so	OK
2026-01-03 06:28:47	Analyzing apktool_out/lib/x86_64/libsrpc_android_jni.so	OK

2026-01-03 06:28:47	Analyzing apktool_out/lib/x86_64/librealm-jni.so	OK
2026-01-03 06:28:47	Reading Code Signing Certificate	OK
2026-01-03 06:28:48	Running APKiD 3.0.0	OK
2026-01-03 06:28:51	Detecting Trackers	OK
2026-01-03 06:28:52	Decompiling APK to Java with JADX	OK
2026-01-03 06:29:00	Converting DEX to Smali	OK
2026-01-03 06:29:01	Code Analysis Started on - java_source	OK
2026-01-03 06:29:02	Android SBOM Analysis Completed	OK
2026-01-03 06:29:05	Android SAST Completed	OK
2026-01-03 06:29:05	Android API Analysis Started	OK
2026-01-03 06:29:06	Android API Analysis Completed	OK

2026-01-03 06:29:07	Android Permission Mapping Started	OK
2026-01-03 06:29:09	Android Permission Mapping Completed	OK
2026-01-03 06:29:09	Android Behaviour Analysis Started	OK
2026-01-03 06:29:11	Android Behaviour Analysis Completed	OK
2026-01-03 06:29:12	Extracting Emails and URLs from Source Code	OK
2026-01-03 06:29:15	Email and URL Extraction Completed	OK
2026-01-03 06:29:15	Extracting String data from APK	OK
2026-01-03 06:29:15	Extracting String data from SO	OK
2026-01-03 06:29:15	Extracting String data from Code	OK
2026-01-03 06:29:15	Extracting String values and entropies from Code	OK

2026-01-03 06:29:17	Performing Malware check on extracted domains	OK
2026-01-03 06:29:21	Saving to Database	OK

Report Generated by - MobSF v4.4.4

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.