MOBSF

ANDROID STATIC ANALYSIS REPORT

Elysai (4.0.3)

File Name:	Elysai_ Talk to AI Friends_4.0.3_Apkpure.apk
Package Name:	ai.flowstorm.poppy
Scan Date:	April 14, 2024, 4:08 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	14	1	2	2

FILE INFORMATION

File Name: Elysai_ Talk to AI Friends_4.0.3_Apkpure.apk
Size: 60.14MB
MD5: 3dff77c714b3f28ca4cd9fefd8cae5ee
SHA1: ea0172d0aa5a76423078207ba7270745f66ce73b
SHA256: 1dcc40a665735e8b829f65aa9353cf664bd93c0b5bb9a09a0bec965fdbc9fc2c

APP INFORMATION

App Name: Elysai
Package Name: ai.flowstorm.poppy
Main Activity: ai.promethist.elysai.ui.activity.StartActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 4.0.3

Android Version Code: 155

APP COMPONENTS

Activities: 8
Services: 9
Receivers: 11
Providers: 4
Exported Activities: 1
Exported Services: 1
Exported Receivers: 3
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: 2021-04-09 14:03:25+00:00
Valid To: 2051-04-09 14:03:25+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x45bdef2ae6eeb2c97a968a753449991edc4bb403
Hash Algorithm: sha256
md5: 9200e3331269d6f48d05823a15ecba05
sha1: bb5f428233f01186693f509942e977903108c1a4
sha256: ddc26f7d663ccfdec6e6b69fed2ccffc65120d0fcb19c077074a70c1cabdc5e0
sha512: 570a207e75b65041098996e83ac3f0ea208abdc4b2e4fb5823f2f44b2cae6f902c6fdb088d0220ab212447b6adb490b8de2f92cca71e7a36f3774f1c970917fb
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ff9f47adaf77baf4d41144b7719c1c3c8600dd87d9a263f0f0ff298961426b2a
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
ai.flowstorm.poppy.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes2.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes6.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes7.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes8.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes9.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: 0 | WARNING: 6 | 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	Activity (ai.promethist.elysai.ui.MainActivity) 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.
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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
4	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.
5	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.
6	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
				ai/flowstorm/client/SimpleClientCallback.java ai/flowstorm/client/gps/NMEA.java ai/flowstorm/client/io/WavFileAudioRecorder.java ai/flowstorm/client/signal/SignalProcessProvider.java ai/flowstorm/client/signal/SignalProcessor$Companion$test$1$1.java ai/flowstorm/client/util/InetInterface.java ai/flowstorm/common/AppConfig.java ai/flowstorm/common/client/HttpPollingSocketClient.java ai/flowstorm/common/monitoring/LoggerMonitoring.java ai/flowstorm/core/model/JobLog.java ai/flowstorm/util/Stack.java ai/promethist/elysai/RedirectLogOutputStream.java ai/promethist/elysai/ui/MainActivity.java ai/promethist/elysai/util/AndroidLog.java ai/promethist/elysai/util/ElysaiRecognitionListener.java ai/promethist/elysai/util/NotificationSchedule.java ai/promethist/elysai/util/VideoProvider$createLocalFileVideoPlayer$1$2.java ch/qos/logback/classic/net/SimpleSocketServer.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/selector/servlet/ContextDetachingSCL.java ch/qos/logback/classic/spi/PackagingDataCalculator.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/recovery/ResilientOutputStreamBase.java ch/qos/logback/core/spi/ContextAwareBase.java ch/qos/logback/core/spi/ContextAwareImpl.java ch/qos/logback/core/subst/Node.java

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	com/ctc/wstx/compat/QNameCreator.java com/ctc/wstx/shaded/msv_core/datatype/regexp/REUtil.java com/ctc/wstx/shaded/msv_core/datatype/regexp/RangeToken.java com/ctc/wstx/shaded/msv_core/driver/textui/ReportErrorHandler.java com/ctc/wstx/shaded/msv_core/reader/xmlschema/XMLSchemaReader.java com/ctc/wstx/shaded/msv_core/scanner/dtd/DTDParser.java com/ctc/wstx/shaded/msv_core/verifier/Verifier.java com/ctc/wstx/shaded/msv_core/verifier/identity/FieldMatcher.java com/ctc/wstx/shaded/msv_core/verifier/identity/FieldsMatcher.java com/ctc/wstx/shaded/msv_core/verifier/identity/IDConstraintChecker.java com/ctc/wstx/shaded/msv_core/verifier/identity/SelectorMatcher.java com/ctc/wstx/shaded/msv_core/verifier/regexp/ContentModelAcceptor.java com/ctc/wstx/shaded/msv_core/verifier/regexp/ExpressionAcceptor.java com/ctc/wstx/shaded/msv_core/verifier/regexp/xmlschema/XSAcceptor.java com/ctc/wstx/shaded/msv_core/writer/relaxng/PatternWriter.java com/ctc/wstx/sw/EncodingXmlWriter.java com/drew/imaging/ImageMetadataReader.java com/drew/lang/CompoundException.java com/drew/tools/ExtractJpegSegmentTool.java com/drew/tools/ProcessAllImagesInFolderUtility.java com/drew/tools/ProcessUrlUtility.java com/goxr3plus/streamplayer/application/AnotherStreamPlayerListener.java com/goxr3plus/streamplayer/application/DemoApplication.java com/goxr3plus/streamplayer/tools/TimeTool.java com/jamal/composeprefs3/ui/prefs/CheckBoxPrefKt$

NO	ISSUE	SEVERITY	STANDARDS	FILES
				CheckBoxPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/DropDownPrefKt$DropDownPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/EditTextPrefKt$EditTextPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/ListPrefKt$ListPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/MultiSelectListPrefKt$MultiSelectListPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/SliderPrefKt$SliderPref$edit$1$1.java com/jamal/composeprefs3/ui/prefs/SwitchPrefKt$SwitchPref$edit$1$1.java com/jcraft/jogg/Buffer.java com/jcraft/jorbis/ChainingExample.java com/jcraft/jorbis/DecodeExample.java com/mikepenz/aboutlibraries/Libs.java com/mikepenz/aboutlibraries/LibsBuilder.java com/mikepenz/aboutlibraries/LibsFragmentCompat.java com/mikepenz/fastadapter/FastAdapter.java com/mikepenz/fastadapter/VerboseLogger.java com/mikepenz/fastadapter/listeners/OnBindViewHolderListenerImpl.java com/sun/jna/Native.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/transport/StdoutTransport.java javax/xml/bind/helpers/DefaultValidationEventHandler.java javax/xml/stream/FactoryFinder.java javazoom/jl/converter/jlc.java javazoom/jl/player/PlayerApplet.java javazoom/jl/player/advanced/jlap.java javazoom/jl/player/jlp.java javazoom/spi/mpeg/sampled/convert/DecodedMpegAudioInputStream.java javazoom/spi/mpeg/sampled/file/tag/IcyInputStream.java junit/runner/BaseTestRunner.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				junit/runner/Version.java junit/textui/TestRunner.java org/glassfish/hk2/osgiresourcelocator/ServiceLoaderImpl.java org/jaudiotagger/Test.java org/jaudiotagger/audio/mp4/Mp4AtomTree.java org/jaudiotagger/audio/mp4/atom/Mp4StcoBox.java org/jaudiotagger/audio/ogg/OggFileReader.java org/jaudiotagger/audio/wav/WavCleaner.java org/jaudiotagger/tag/images/StandardImageHandler.java org/jaudiotagger/test/ExtractID3TagFromFile.java org/jaudiotagger/test/MergeID3AndMP3Files.java org/jaudiotagger/test/TestAudioTagger.java org/jaudiotagger/utils/FileTypeUtil.java org/jflac/frame/EntropyPartitionedRice.java org/jflac/io/RandomFileInputStream.java org/jflac/util/RingBuffer.java org/slf4j/helpers/Util.java org/tritonus/lowlevel/cdda/cooked_ioctl/CookedIoctl.java org/tritonus/lowlevel/gsm/GSMDecoder.java org/tritonus/lowlevel/gsm/Gsm_State.java org/tritonus/sampled/mixer/alsa/AlsaPortMixerProvider.java
				ai/flowstorm/channel/event/InitEvent.java ai/flowstorm/common/monitoring/SentryMonitoring.java ai/flowstorm/common/monitoring/User.java ai/flowstorm/core/ClientConfig.java ai/flowstorm/core/Request.java ai/flowstorm/core/model/Property.java ai/flowstorm/core/nlp/pipeline/PipelineConfig.java ai/promethist/elysai/model/command/User.java ai/promethist/elysai/ui/activity/ProfileActivity.java ai/promethist/elysai/util/Preferences.java ch/qos/logback/classic/ClassicConstants.java ch/qos/logback/classic/gaffer/GafferConfigurator.java ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	.java ch/qos/logback/classic/sift/JNDIBasedContextDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/db/BindDataSourceToJNDIAction.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 coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java com/auth0/jwk/GuavaCachedJwkProvider.java com/ctc/wstx/shaded/msv_core/reader/trex/ng/RELAXNGReader.java com/ctc/wstx/shaded/msv_core/reader/xmlschema/XMLSchemaReader.java com/ctc/wstx/shaded/msv_core/verifier/identity/IDConstraintChecker.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java io/sentry/RequestDetailsResolver.java org/glassfish/jersey/SslConfigurator.java org/glassfish/jersey/internal/l10n/Localizer.java org/jaudiotagger/tag/id3/ID3v22Frames.java org/jaudiotagger/tag/id3/ID3v23Frames.java org/jaudiotagger/tag/id3/ID3v24Frames.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	ai/flowstorm/security/Digest.java gnu/trove/TByteArrayList.java gnu/trove/TDoubleArrayList.java gnu/trove/TFloatArrayList.java gnu/trove/TIntArrayList.java gnu/trove/TLongArrayList.java org/junit/runner/manipulation/Ordering.java org/tritonus/lowlevel/dsp/PinkNoise.java org/tritonus/lowlevel/dsp/WhiteNoise.java org/tritonus/sampled/convert/pvorbis/VorbisFormatConversionProvider.java org/tritonus/sampled/convert/vorbis/VorbisFormatConversionProvider.java org/tritonus/share/sampled/FloatSampleTools.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	ai/flowstorm/security/Digest.java com/adobe/internal/xmp/impl/XMPUtilsImpl.java
5	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/promethist/elysai/util/AudioPlayer.java coil/decode/SourceImageSource.java com/sun/jna/Native.java org/glassfish/jersey/message/internal/FileProvider.java org/glassfish/jersey/message/internal/Utils.java org/jaudiotagger/audio/generic/AudioFileWriter.java org/jaudiotagger/tag/id3/AbstractID3v2Tag.java org/junit/rules/TemporaryFolder.java
6	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 org/glassfish/jersey/SslConfigurator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/DefaultAndroidEventProcessor.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/util/RootChecker.java
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/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: ['__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_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: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__vsnprintf_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: ['__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_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: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__vsnprintf_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

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/45	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, 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
www.shoutcastserver.com	IP: 154.205.99.42 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.tritonus.org	ok	**IP:** 138.201.54.42 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.thaiopensource.com	ok	**IP:** 119.81.18.13 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.javazoom.net	ok	No Geolocation information available.
www.server.com	ok	**IP:** 52.8.126.80 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **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

DOMAIN	STATUS	GEOLOCATION
www.sun.com	ok	**IP:** 23.53.4.27 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
xml.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
musicbrainz.org	ok	**IP:** 142.132.240.1 **Country:** Canada **Region:** Manitoba **City:** Winnipeg **Latitude:** 49.889748 **Longitude:** -97.153961 **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

DOMAIN	STATUS	GEOLOCATION
core-elysai-preview.flowstorm.ai	ok	**IP:** 104.26.8.152 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
core-preview.flowstorm.ai	ok	**IP:** 104.26.8.152 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
relaxng.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
java.sun.com	ok	**IP:** 23.53.4.27 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
ns.useplus.org	ok	**IP:** 54.83.4.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
core.flowstorm.ai	ok	**IP:** 104.26.8.152 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.aiim.org	ok	**IP:** 199.60.103.225 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s3.eu-central-1.amazonaws.com	ok	**IP:** 52.219.169.193 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
core-elysai.flowstorm.ai	ok	**IP:** 104.26.8.152 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.111.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
iptc.org	ok	**IP:** 3.64.29.21 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
yaml.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.iso-relax.org	ok	No Geolocation information available.
repository.flowstorm.ai	ok	**IP:** 172.67.71.153 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
zayda.eu.ngrok.io	ok	**IP:** 3.17.7.232 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
www.npes.org	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
www.shoutcastserver.com	ok	**IP:** 154.205.99.42 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
www.xml.gr.jp	ok	**IP:** 49.212.36.76 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
cipa.jp	ok	**IP:** 118.82.81.189 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
promethist.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
drewnoakes.com	ok	**IP:** 34.229.76.186 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.elysai.com	ok	**IP:** 34.149.87.45 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.apple.com	ok	**IP:** 23.223.216.31 **Country:** France **Region:** Ile-de-France **City:** Aubervilliers **Latitude:** 48.916672 **Longitude:** 2.383330 **View:** Google Map
purl.org	ok	**IP:** 207.241.239.241 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
play.google.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xerces.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
mikepenz.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.id3.org	ok	**IP:** 167.99.106.11 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://promethist.firebaseio.com/.json	high Firebase DB is exposed publicly.

EMAILS

EMAIL	FILE
support@elysai.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBkwcaAK5dSFqjda2YPMWFOOGJMypG-4lU"
"library_AboutLibraries_authorWebsite" : "http://mikepenz.com/"
"google_crash_reporting_api_key" : "AIzaSyBkwcaAK5dSFqjda2YPMWFOOGJMypG-4lU"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"

POSSIBLE SECRETS
"firebase_database_url" : "https://promethist.firebaseio.com"
6486cb2f8af625324033ea9e
013602400437880159360205O5
e2719d58-a985-b3c9-781a-b030af78d30e
648724376ab74917ac641788
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
6486cb426ab74917ac5eef04
6483253f8af62532402ef021
49f946663a8deb7054212b8adda248c6
648723c86ab74917ac63e62d
646b32029878b4484e1dce3b
9a04f079-9840-4286-ab92-e65be0885f95
648724256ab74917ac641778
632af932091b903bd1ba601b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

POSSIBLE SECRETS
c103703e120ae8cc73c9248622f3cd1e
64ad211ef3a1040e23386b12
6486cb188af625324033e900
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
64ef37ff35094e2b1ee0d962
648324fb8af62532402edf9d

PLAYSTORE INFORMATION

Title: Elysai: Talk to AI Friends

Score: 4.18 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** ai.flowstorm.poppy

Developer Details: PromethistAI a.s., 5442656805872185667, None, https://www.elysai.com/, info@elysai.com,

Release Date: Apr 9, 2021 **Privacy Policy:** Privacy link

Description:

Meet the first AI-powered Digital Personas that teach you the art of life satisfaction. Talk with them to learn how to work with your emotions and perceptions and live a better life each day. You can talk freely about your everyday issues or just release tension and unwind. Here, anyone can openly share their feelings, get support and learn more about themselves. Our Digital Personas are socially intelligent virtual beings who were created at the intersection of well-being and entertainment. The combination of our cutting-edge conversational AI technology and psychological research enables the Digital Personas to have complex and truly engaging conversations while being more humanlike and better suited to people’s needs for communication, trust and comfort. Enjoy the exciting experience of talking with an AI who is able to recognize human moods and learns more about the world of feelings and emotions from each conversation. Every user's needs are different – and so are the interactions.

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.