MOBSF

ANDROID STATIC ANALYSIS REPORT

ERG 2024 (4.1.1)

File Name:	gov.nih.nlm.erg2012_25.apk
Package Name:	gov.nih.nlm.erg2012
Scan Date:	Sept. 1, 2025, 1:23 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	16	2	1	1

FILE INFORMATION

File Name: gov.nih.nlm.erg2012_25.apk
Size: 50.1MB
MD5: 4fabb5725238356acde4de268b5cbf14
SHA1: 70f71761f7467017ff07d62b32544e5ce60f7bee
SHA256: 771401a367eddd7542138ae9a83f671aad8c8f622b6595e8e58aa4a9c90c2d7c

APP INFORMATION

App Name: ERG 2024
Package Name: gov.nih.nlm.erg2012
Main Activity: gov.nih.nlm.erg2012.Erg2024Launcher
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 4.1.1
Android Version Code: 25

APP COMPONENTS

Activities: 17
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 11
Exported Services: 0
Exported Receivers: 0
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=Maryland, L=Bethesda, O=Department of Health and Human Services, OU=National Institutes of Health, CN=National Library of Medicine
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-08-05 15:59:49+00:00
Valid To: 2038-12-21 15:59:49+00:00
Issuer: C=US, ST=Maryland, L=Bethesda, O=Department of Health and Human Services, OU=National Institutes of Health, CN=National Library of Medicine
Serial Number: 0x4e3c1375
Hash Algorithm: sha1
md5: a589065eed388f8182c1c45de8454885
sha1: 9fa481eda08b7acfd6384ae5b5b9c0ddf29286b3
sha256: abf5b2260c5ac467d1073b1c5f869eee954b279e7c6e305fccad7ed0aaa7d9b3
sha512: f2d48d230acc0ac0980ea59ad81a93d39f63b252a2606e62bb4c75db172ebaea0f5a8b76283f93a4a1888a4f83a1319b67509f658806bb9712a015d56ec4f4d7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b4d8dc96d85e13bd5180fc4e180aede480e2c75d8a3b2cf9e5d4ad514255d4d9
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	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</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>classes2.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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
gov.nih.nlm.wiser.common.link.LinkDispatcherActivity	Schemes: http://, https://, Hosts: @string/AppDomain, Path Prefixes: /erg,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 12 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (gov.nih.nlm.wiser.common.link.LinkDispatcherActivity) 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	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.ErgHomeActivity) 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.
5	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.searchMaterials.SearchMaterialActivity) 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	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.settings.ErgSettingsActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.about.AboutActivity) 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.
8	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.guidePageViewer.GuidePageViewer) 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.
9	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.map.ErgMapActivity) 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.
10	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.referenceMaterialViewer.ErgReferenceMaterialViewer) 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.
11	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.referenceViewer.NotificationViewer) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.bleve.BleveActivity) 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.
13	Activity (gov.nih.nlm.wiser.common.guiLayer.tools.erg.ied.IedActivity) 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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 2 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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

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	cher.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/jaredrummler/android/colorpicker/ColorPickerDialog.java gov/nih/nlm/utility/dataAccess/dao/AbstractDAO.java gov/nih/nlm/utility/dataAccess/util/DatabaseHelper.java gov/nih/nlm/utility/dataAccess/util/DbUtil.java gov/nih/nlm/utility/dataAccess/util/FormatUtil.java gov/nih/nlm/utility/dataAccess/util/ZipUtil.java gov/nih/nlm/utility/guiLayer/util/SectionAdapter.java gov/nih/nlm/wiser/common/UniversalApplication.java gov/nih/nlm/wiser/common/dataAccess/dao/DatabaseVersionDAO.java gov/nih/nlm/wiser/common/dataAccess/dao/ErgImageDAO.java gov/nih/nlm/wiser/common/dataAccess/data/ErgImage.java gov/nih/nlm/wiser/common/dataAccess/data/ErgMaterial.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/ErgHomeActivity.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/ErgManager.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/about/AboutActivity.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/ergSearchByImage/ErgImageListAdapter.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/guidePageViewer/GuidePageFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gov/nih/nlm/wiser/common/guiLayer/tools/erg/guidePageViewer/GuidePageViewer.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/logic/formatters/ErgHtmlFormatter.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/ErgProtectiveZone.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/MapLocationFragment.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/NotifyTracker.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/UniversalSettings.java gov/nih/nlm/wiser/common/guiLayer/tools/referenceViewer/ReferenceDocumentFragment.java gov/nih/nlm/wiser/common/guiLayer/util/LocalizedNumberExtractionFormatter.java gov/nih/nlm/wiser/common/link/AbstractLinkHandler.java gov/nih/nlm/wiser/common/link/ErgMaterialChooserFragment.java gov/nih/nlm/wiser/common/link/LinkDispatcherActivity.java gov/nih/nlm/wiser/common/link/ProtectiveDistanceLinkHandler.java gov/nih/nlm/wiser/referenceEngine/dao/ReferenceDocumentImageDAO.java gov/nih/nlm/wiser/referenceEngine/data/ReferenceDocument.java gov/nih/nlm/wiser/referenceEngine/guiLayer/RefDocFragment.java gov/nih/nlm/wiser/referenceEngine/guiLayer/ReferenceWebViewClient.java javax/xml/bind/helpers/DefaultValidationEventHandler.java javax/xml/stream/FactoryFinder.java
2	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	gov/nih/nlm/erg2012/Erg2024Launcher.java gov/nih/nlm/wiser/referenceEngine/guiLayer/RefDocFragment.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	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 gov/nih/nlm/utility/VersionedSerializationKey.java gov/nih/nlm/utility/guiLayer/util/ErrorReporter.java gov/nih/nlm/wiser/common/dataAccess/dao/ErgMaterialDAO.java gov/nih/nlm/wiser/common/dataAccess/dao/ErgTable3DistanceDAO.java gov/nih/nlm/wiser/common/dataAccess/data/ErgIed.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/ErgProtectiveZoneKt.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/LocationHistoryKt.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/referenceMaterialViewer/ErgReferenceMaterialViewer.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/searchMaterials/MaterialHistory.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/searchMaterials/SearchMaterialActivity.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/searchMaterials/SearchMaterialFragment.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/ErgSettings.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/NotifyTracker.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/UniversalSettings.java gov/nih/nlm/wiser/common/guiLayer/tools/referenceViewer/ReferenceDocumentFragment.java gov/nih/nlm/wiser/common/guiLayer/tools/referenceViewer/ReferenceTopicFragment.java gov/nih/nlm/wiser/referenceEngine/data/ReferenceDocument.java gov/nih/nlm/wiser/referenceEngine/data/ReferenceTopic.java gov/nih/nlm/wiser/referenceEngine/data/ReferenceTopicTy

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pe.java gov/nih/nlm/wiser/referenceEngine/guiLayer/RefDocFragment.java gov/nih/nlm/wiser/referenceEngine/guiLayer/RefTopicFragment.java
4	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/ErgProtectiveZone.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/map/MapActivity.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/settings/ErgSettingsSectionAdapter.java
5	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	gov/nih/nlm/utility/guiLayer/util/BasicWebView.java
6	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	gov/nih/nlm/utility/guiLayer/util/BasicWebView.java

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	com/ctc/wstx/dtd/DTDSchemaFactory.java com/ctc/wstx/shaded/msv/org_isorelax/jaxp/ValidatingSAXParser.java com/ctc/wstx/shaded/msv_core/scanner/dtd/Resolver.java com/ctc/wstx/stax/WstxInputFactory.java com/ctc/wstx/util/URLUtil.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java javax/activation/FileDataSource.java javax/xml/bind/helpers/AbstractUnmarshallerImpl.java javax/xml/stream/FactoryFinder.java org/codehaus/stax2/io/Stax2FileSource.java org/codehaus/stax2/io/Stax2URLSource.java org/codehaus/stax2/validation/XMLValidationSchemaFactory.java
00022	Open a file from given absolute path of the file	file	com/ctc/wstx/shaded/msv/org_isorelax/verifier/VerifierFactory.java com/ctc/wstx/shaded/msv/org_isorelax/verifier/impl/VerifierImpl.java com/ctc/wstx/shaded/msv_core/scanner/dtd/Resolver.java com/ctc/wstx/shaded/msv_core/util/Util.java com/ctc/wstx/util/URLUtil.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java
00091	Retrieve data from broadcast	collection	gov/nih/nlm/wiser/common/guiLayer/tools/erg/ErgHomeActivity.java gov/nih/nlm/wiser/common/guiLayer/tools/erg/searchMaterials/SearchMaterialActivity.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00012	Read data and put it into a buffer stream	file	javax/xml/bind/helpers/AbstractUnmarshallerImpl.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	gov/nih/nlm/wiser/common/guiLayer/tools/referenceViewer/ReferenceWebViewClient.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	0/44	

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
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
java.sun.com	ok	**IP:** 23.62.226.28 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.iso-relax.org	ok	No Geolocation information available.
www.sun.com	ok	**IP:** 23.62.226.2 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
www.phmsa.dot.gov	ok	**IP:** 2.19.152.156 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
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
relaxng.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
ergcomments@dot.gov	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"Biblio_AuthorSep" : ", "
"Biblio_AuthorSuffix" : ". "
013602400437880159360205O5

PLAYSTORE INFORMATION

Title: ERG for Android

Score: 4.34 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** gov.nih.nlm.erg2012

Developer Details: PHMSA, PHMSA, None, http://www.phmsa.dot.gov/hazmat/outreach-training/erg, training@dot.gov,

Release Date: Jan 8, 2013 **Privacy Policy:** Privacy link

Description:

PHMSA's Emergency Response Guidebook (ERG) is the go-to resource for first responders during the initial phase of a dangerous goods or hazardous materials transportation incident. The ERG app is a valuable companion, based on the latest edition of the ERG, to help responders quickly access critical information at their fingertips. The app features an indexed list of dangerous goods, including their associated ID number, general hazards, and recommended safety precautions. In practical scenarios, such as responding to an overturned tractor trailer displaying a DOT hazmat placard, emergency responders can use the app to quickly identify the material associated with the placard and get guidance on how to respond effectively. Full versions available in English, French, and Spanish.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:23:35	Generating Hashes	OK

2025-09-01 13:23:36	Extracting APK	OK
2025-09-01 13:23:36	Unzipping	OK
2025-09-01 13:23:37	Parsing APK with androguard	OK
2025-09-01 13:23:37	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:23:37	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:23:39	Parsing AndroidManifest.xml	OK
2025-09-01 13:23:39	Extracting Manifest Data	OK
2025-09-01 13:23:39	Manifest Analysis Started	OK
2025-09-01 13:23:39	Performing Static Analysis on: ERG 2024 (gov.nih.nlm.erg2012)	OK
2025-09-01 13:23:41	Fetching Details from Play Store: gov.nih.nlm.erg2012	OK
2025-09-01 13:23:42	Checking for Malware Permissions	OK

2025-09-01 13:23:42	Fetching icon path	OK
2025-09-01 13:23:42	Library Binary Analysis Started	OK
2025-09-01 13:23:42	Reading Code Signing Certificate	OK
2025-09-01 13:23:43	Running APKiD 2.1.5	OK
2025-09-01 13:23:47	Detecting Trackers	OK
2025-09-01 13:23:49	Decompiling APK to Java with JADX	OK
2025-09-01 13:24:01	Converting DEX to Smali	OK
2025-09-01 13:24:01	Code Analysis Started on - java_source	OK
2025-09-01 13:24:03	Android SBOM Analysis Completed	OK
2025-09-01 13:24:06	Android SAST Completed	OK
2025-09-01 13:24:06	Android API Analysis Started	OK

2025-09-01 13:24:09	Android API Analysis Completed	OK
2025-09-01 13:24:09	Android Permission Mapping Started	OK
2025-09-01 13:24:11	Android Permission Mapping Completed	OK
2025-09-01 13:24:11	Android Behaviour Analysis Started	OK
2025-09-01 13:24:14	Android Behaviour Analysis Completed	OK
2025-09-01 13:24:14	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:24:16	Email and URL Extraction Completed	OK
2025-09-01 13:24:16	Extracting String data from APK	OK
2025-09-01 13:24:16	Extracting String data from Code	OK
2025-09-01 13:24:16	Extracting String values and entropies from Code	OK
2025-09-01 13:24:18	Performing Malware check on extracted domains	OK

2025-09-01 13:24:20	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.