

ANDROID STATIC ANALYSIS REPORT



Vietnam Health Declaration (Failed)

File Name: Vietnam Health Declaration 1.0.12.apk

Package Name: Failed

Average CVSS Score: 6.4

App Security Score: 50/100 (MEDIUM RISK)

Trackers Detection: 1/285



File Name: Vietnam Health Declaration 1.0.12.apk

Size: 5.86MB

MD5: c72f5bd481177980285b0de00eb52bff

SHA1: caa9eca7c0266c2e1db6d42ec3d825ebdb84b7b3

SHA256: b24a3a47f1bf3be1146f732eeef4551970aea9aba8681748e7f1d8b60e0a8be1

1 APP INFORMATION

App Name: Vietnam Health Declaration

Package Name: Failed

Main Activity: Target SDK: Min SDK: Max SDK:

Android Version Name: Failed Android Version Code: Failed

APP COMPONENTS

Activities: 0 Services: 0 Receivers: 0

Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

***** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: True v3 signature: True

Found 1 unique certificates

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

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-03-05 15:01:10+00:00 Valid To: 2050-03-05 15:01:10+00:00

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

Serial Number: 0x159e6656641a473cd223ed6896f46437fca52386

Hash Algorithm: sha256

md5: a95dccf1e3c53bcc3c118f5316a95246

sha1: 9810440c5e939d1f48cdc21ddd401e358e4d202d

sha256: c0d15e198d21f09f82ab141366453a4b7dc451e10230291d50f1f796bbcbe057

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 0084e25c218294b0a7759c517d234f1054adecb27fa30155a2d530fd211fe4d9

Certificate Status: Good

Description: Certificate looks good.

ক্ল APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes10.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes11.dex	Compiler	dx	
classes12.dex	FINDINGS	DETAILS	
5,000,000	Compiler	dx	
	FINDINGS	DETAILS	
classes13.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes14.dex	Compiler	dx	
		Ţ Ţ	
classes15.dex	FINDINGS	DETAILS	
	Compiler	dx	

FILE	DETAILS		
classes16.dex	FINDINGS	DETAILS	
	Compiler	dx	
classes17.dex	FINDINGS	DETAILS	
	Compiler	dx	
classes18.dex	FINDINGS	DETAILS	
	Compiler	dx	
classes19.dex	FINDINGS	DETAILS	
	Compiler	dx	
classes2.dex	FINDINGS	DETAILS	
Clussesztack	Compiler	dx	
classes20.dex	FINDINGS	DETAILS	
Classeszo.ucx	Compiler	dx	
classes21.dex	FINDINGS	DETAILS	
Clusses21.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes22.dex	Compiler	dx	
classes23.dex	FINDINGS	DETAILS	
	Compiler	dx	

FILE	DETAILS		
dance 24 days	FINDINGS	DETAILS	
classes24.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes25.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes26.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes27.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes28.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes29.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes3.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes30.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes31.dex	Compiler	dx	

FILE	DETAILS			
classes32.dex	FINDINGS		DETAILS	
Classes32.uex	Compiler		dx	
	FINDINGS		DETAILS	
classes33.dex	Compiler		dx	
	FINDINGS		DETAILS	
classes34.dex	Compiler		dx	
	FINDINGS		DETAILS	
classes35.dex	Compiler		dx	
			DETAILS	
classes36.dex	FINDINGS Compiler		dx	
	FINDINGS		DETAILS	
classes37.dex	Compiler		dx	
Classessy, acx				
	FINDINGS		DETAILS	
classes38.dex	Compiler		dx	
	FINDINGS	DETAILS		
classes39.dex	Anti Debug Code	Debug.isDebugger(Connected() check	
	Compiler	dx		

FILE	DETAILS		
classes4.dex	FINDINGS	DETAILS	
Classes4.uex	Compiler	dx	
	FINDINGS	DETAILS	
classes40.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes41.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes42.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes43.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes44.dex	Compiler	dx	
classes45.dex	FINDINGS	DETAILS	
Classes+J.deA	Compiler	dx	
classes46.dex	FINDINGS	DETAILS	
	Compiler	dx	
	FINDINGS	DETAILS	
classes47.dex	Compiler	dx	

FILE	DETAILS		
description of the second	FINDINGS	DETAILS	
classes48.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes49.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes5.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes50.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes51.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes52.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes53.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes54.dex	Compiler	dx	
	FINDINGS	DETAILS	
classes55.dex	Compiler	dx	

FILE	DETAILS					
classes56.dex	FINDINGS Compiler		DETAILS dx			
	FINDINGS	DETAILS				
classes57.dex	Build.PRODUCT		EL check JFACTURER check UCT check	DEL check IUFACTURER check	k JRER check Jeck	
	Compiler	dx				
classes58.dex	FINDINGS		DETAILS	DETAILS		
Classespoluex	Compiler		dx	dx		
	FINDINGS DETAILS					
classes59.dex	Compiler unknown (please file det		file detection issue!)	e file detection issue!)		
classes6.dex	FINDINGS		DETAILS	DETAILS		
	Compiler		dx	dx		
classes60.dex	FINDINGS		DETAILS	DETAILS		
Classesociaex	Compiler		dx	dx		
classes61.dex	FINDINGS		DETAILS	DETAILS		
Classes01.uex	Compiler		dx	dx		
classes62.dex	FINDINGS		DETAILS	DETAILS		
Classes02.uex	Compiler		dx	dx		

FILE	DETAILS		
	FINDINGS	DETAILS	
classes7.dex	Compiler	dx	
classes8.dex	FINDINGS	DETAILS	
	Compiler	dx	
classes9.dex	FINDINGS	DETAILS	
Classes	Compiler	dx	

Q MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
-------	----------	-----------	-------

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	cordova/plugins/screenorientation/CD VOrientation.java org/slf4j/helpers/Util.java ch/qos/logback/core/net/SocketConne ctorBase.java ch/qos/logback/core/net/DefaultSocke tConnector.java ch/qos/logback/core/recovery/Resilie ntOutputStreamBase.java ch/qos/logback/core/joran/util/Config urationWatchListUtil.java ch/qos/logback/core/spi/ContextAwar eBase.java ch/qos/logback/core/spi/ContextAwar elmpl.java ch/qos/logback/core/spi/ContextAwar elmpl.java ch/qos/logback/core/subst/Node.java ch/qos/logback/classic/net/SimpleSoc ketServer.java ch/qos/logback/classic/spi/Throwable Proxy.java ch/qos/logback/classic/android/Logca tAppender.java ch/qos/logback/classic/pattern/Target LengthBasedClassNameAbbreviator.ja va me/leolin/shortcutbadger/ShortcutBa dger.java com/intentfilter/androidpermissions/ helpers/Logger.java com/adobe/phonegap/push/PushPlug in.java com/adobe/phonegap/push/PushPlug in.java com/adobe/phonegap/push/PushDis missedHandler.java com/adobe/phonegap/push/PushInst ancelDListenerService.java com/adobe/phonegap/push/PushHan dlerActivity.java com/adobe/phonegap/push/PushHan dlerActivity.java com/marianhello/bgloc/BootComplet edReceiver.java com/marianhello/bgloc/BootComplet edReceiver.java com/marianhello/bgloc/data/sqlite/S QLiteOpenHelper.java com/marianhello/bgloc/data/sqlite/S QLiteOpenHelper.java com/phonegap/plugins/barcodescann er/BarcodeScanner.java

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	org/slf4j/helpers/SubstituteLogger.jav a org/slf4j/helpers/BasicMarker.java ch/qos/logback/core/joran/spi/Eleme ntSelector.java ch/qos/logback/core/joran/spi/HostCl assAndPropertyDouble.java ch/qos/logback/core/status/StatusBas e.java ch/qos/logback/core/spi/AbstractCom ponentTracker.java ch/qos/logback/core/pattern/parser/F ormattingNode.java ch/qos/logback/core/pattern/parser/N ode.java ch/qos/logback/core/pattern/parser/C ompositeNode.java ch/qos/logback/core/pattern/parser/T oken.java ch/qos/logback/core/pattern/parser/Si mpleKeywordNode.java ch/qos/logback/core/subst/Node.java ch/qos/logback/core/subst/Token.java ch/qos/logback/core/subst/Token.java ch/qos/logback/classic/spi/ClassPacka gingData.java ch/qos/logback/classic/spi/StackTrace ElementProxy.java ch/qos/logback/classic/spi/LoggingEve ntVO.java ch/qos/logback/classic/spi/LoggingEve ntVO.java ch/qos/logback/classic/spi/LoggingEve ntVO.java com/intentfilter/androidpermissions/ PermissionManager.java com/intentfilter/androidpermissions/s ervices/NotificationService.java com/github/jparkie/promise/extras/P air.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 - Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ch/qos/logback/core/CoreConstants.ja va ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/D ateTokenConverter.java ch/qos/logback/core/rolling/helper/Int egerTokenConverter.java ch/qos/logback/classic/sift/ContextBa sedDiscriminator.java ch/qos/logback/classic/joran/action/C onfigurationAction.java com/adobe/phonegap/push/FCMServi ce.java com/adobe/phonegap/push/PushCon stants.java com/marianhello/bgloc/Config.java com/marianhello/bgloc/Cordova/head less/JsEvaluatorTaskRunner.java com/marianhello/bgloc/data/Abstract LocationTemplate.java

ISSUE	SEVERITY	STANDARDS	FILES
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.	high	CVSS V2: 5.9 (medium) 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/SQLit eAppender.java com/marianhello/bgloc/data/sqlite/S QLiteLocationDAO.java com/marianhello/bgloc/data/sqlite/S QLiteOpenHelper.java com/marianhello/logging/DBLogRead er.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.jav a
Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CVSS V2: 8.8 (high) CWE: CWE-749 - Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/evgenii/jsevaluator/WebViewWra pper.java

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	good	No Geolocation information available.

URLS

URL	FILE
http://www.slf4j.org/codes.html#no_static_mdc_binder http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html http://www.slf4j.org/codes.html#loggerNameMismatch http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#StaticLoggerBinder http://www.slf4j.org/codes.html#null_LF http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#substituteLogger http://www.slf4j.org/codes.html#unsuccessfullnit http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
http://logback.qos.ch/codes.html#null_CS	org/slf4j/impl/StaticLoggerBinder.java
http://logback.qos.ch/codes.html#layoutInsteadOfEncoder	ch/qos/logback/core/OutputStreamAppender.java
http://logback.qos.ch/codes.html http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/CoreConstants.java

URL	FILE
http://logback.qos.ch/codes.html#1andOnly1	ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java
http://logback.qos.ch/codes.html#syslog_layout	ch/qos/logback/core/net/SyslogAppenderBase.java
http://logback.qos.ch/codes.html#socket_no_port http://logback.qos.ch/codes.html#socket_no_host	ch/qos/logback/core/net/AbstractSocketAppender.java
http://logback.qos.ch/codes.html#smtp_no_layout	ch/qos/logback/core/net/SMTPAppenderBase.java
http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java
http://logback.qos.ch/codes.html#tbr_fnp_prudent_unsupported http://logback.qos.ch/codes.html#fwrp_parentFileName_not_set http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java
http://logback.qos.ch/codes.html#sbtp_size_format	ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java
http://logback.qos.ch/codes.html#rfa_collision http://logback.qos.ch/codes.html#rfa_no_rp http://logback.qos.ch/codes.html#rfa_no_tp http://logback.qos.ch/codes.html#rfa_file_after	ch/qos/logback/core/rolling/RollingFileAppender.java
http://logback.qos.ch/codes.html#renamingError	ch/qos/logback/core/rolling/helper/RenameUtil.java
http://logback.qos.ch/codes.html#appender_order	ch/qos/logback/core/joran/action/AppenderRefAction.java
http://xml.org/sax/features/validation http://xml.org/sax/features/namespaces	ch/qos/logback/core/joran/event/SaxEventRecorder.java
http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd	ch/qos/logback/core/html/HTMLLayoutBase.java
http://logback.qos.ch/codes.html#missingRightParenthesis	ch/qos/logback/core/pattern/parser/Parser.java
http://logback.qos.ch/codes.html#receiver_no_port http://logback.qos.ch/codes.html#receiver_no_host	ch/qos/logback/classic/net/SocketReceiver.java
http://logback.qos.ch/css/classic.css	ch/qos/logback/classic/html/UrlCssBuilder.java
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
http://mindprod.com	com/mindprod/ledatastream/LEDataInputStream.java
data:text/html;charset=utf-8;base64,	com/evgenii/jsevaluator/WebViewWrapper.java
https://vhv-office.firebaseio.com	Android String Resource



FIREBASE URL	DETAILS
https://vhv-office.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.

For every findings with severity high we reduce 15 from the score.

For every findings with severity warning we reduce 10 from the score.

For every findings with severity good we add 5 to the score.

If the calculated score is greater than 100, then the app security score is considered as 100.

And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 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.

© 2020 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.