



ANDROID STATIC ANALYSIS REPORT



 Treehouses Remote (5957)

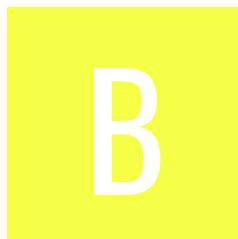
File Name: installer262.apk

Package Name: io.treehouses.remote






Scan Date: May 31, 2022, 9:43 a.m.

App Security Score: 43/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	8	3	1	1

FILE INFORMATION

File Name: installer262.apk

Size: 5.18MB

MD5: f8f97382eeaa57fd76b7b1668309114a

SHA1: 41afba06b3ab22863e08b1a90dc93e7011a6b7a0

SHA256: 15716e2a0fda5f9272f304d85dc90d368b93983a362a1a122af1fb4cd584ae58

APP INFORMATION

App Name: Treehouses Remote

Package Name: io.treehouses.remote

Main Activity: io.treehouses.remote.SplashScreenActivity

Target SDK: 29

Min SDK: 15

Max SDK:

Android Version Name: 5957

Android Version Code: 5957

APP COMPONENTS

Activities: 4
Services: 3
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-23 11:51:12+00:00
Valid To: 2047-12-09 11:51:12+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x2dff9565
Hash Algorithm: sha256
md5: 9e7ecb2d0cc21384f0772e2331574eb7
sha1: fafe247077d89bbf5c1577da4f459b61d01b9010
sha256: 289b409fccbc129101ee19c9981807b47f81a6c62ab996795b9df03be334291b
sha512: 10e27b19d49094c1f97d401153dc9e6de5907ce4c8c7f6cb83588dd3d43c3e22ae57aff6c5bc667ffc7efeecb5ca124f2bec91d6834fe26e47578af150649437

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.ACTION_PICK_WIFI_NETWORK	unknown	Unknown permission	Unknown permission from android reference
android.Manifest.permission.OVERRIDE_WIFI_CONFIG	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
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.
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.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/trilead/ssh2/compression/Zlib.java com/mikepenz/iconics/Iconics.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java com/mikepenz/iconics/IconicsDrawable.java com/parse/ManifestInfo.java com/parse/ConnectivityNotifier.java com/parse/ParseInstallation.java com/mikepenz/fastadapter/listeners/OnBindViewHolderListenerImpl.java c/g/l/h.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	c/g/e/h.java c/p/e.java c/i/h/c.java com/parse/ParseDateFormat.java c/g/l/f.java c/g/e/f.java io/treehouses/remote/views/c/b.java c/g/l/x.java c/g/l/u.java c/g/e/m.java c/g/d/c/b.java com/parse/Parse.java c/g/e/j.java c/g/l/b.java com/parse/InstallationId.java c/q/a/a/h.java com/parse/ParseKeyValueCache.java io/treehouses/remote/j/d.java e/b/a/l.java c/l/a/b.java com/parse/ParsePinningEventuallyQueue.java c/g/d/c/f.java com/mikepenz/fastadapter/FastAdapter.java e/b/a/i.java c/n/a/a.java com/parse/CachedCurrentInstallationController.java c/g/d/c/a.java c/g/j/b.java c/g/l/v.java c/g/e/n.java io/treehouses/remote/d/i.java c/g/l/d0/c.java com/mikepenz/iconics/context/ReflectionUtils.java com/mikepenz/materialdrawer/util/AbstractDrawerImageLoader.java c/p/j0.java c/a/k/a/a.java io/treehouses/remote/e/a.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				me/zhanghai/android/materialprogress bar/MaterialProgressBar.java com/parse/ParseRequest.java com/parse/ParseImpreciseDateFormat.j ava com/mikepenz/iconics/utils/IconicsUtils .java c/g/e/i.java c/g/h/b.java com/parse/NetworkQueryController.jav a e/b/a/b.java c/a/o/g.java c/g/l/c0.java com/parse/ParseObject.java c/r/a/b.java
2	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	io/treehouses/remote/j/c.java
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	io/treehouses/remote/j/c.java e/d/a/j.java com/trilead/ssh2/crypto/digest/HMAC.j ava e/d/a/r/a.java e/d/a/r/d.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	com/parse/ParseRESTCommand.java com/parse/ParseDigestUtils.java e/d/a/j.java com/trilead/ssh2/crypto/digest/HMAC.j ava

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/treehouses/remote/ssh/beans/HostBean.java io/treehouses/remote/d/t.java com/mikepenz/octicons_typeface_library/BuildConfig.java com/mikepenz/fontawesome_typeface_library/BuildConfig.java e/d/a/r/b.java
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	io/treehouses/remote/ssh/beans/HostBean.java io/treehouses/remote/d/n.java io/treehouses/remote/ssh/beans/KnownHostBean.java
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	com/parse/ParseSQLiteDatabase.java com/parse/OfflineSQLiteOpenHelper.java
8	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	g/t/b.java com/parse/LocalIdManager.java g/t/a.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	io/treehouses/remote/h/q.java io/treehouses/remote/e/n.java
10	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/treehouses/remote/h/p.java io/treehouses/remote/utils/n.java io/treehouses/remote/h/r/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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/parse/ParseCommandCache.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	lib/mips/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Partial RELRO warning</p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/mips64/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Partial RELRO warning</p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Partial RELRO warning</p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libpl_droidsonroids_gif.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'bluetooth', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256', 'HMAC-SHA-512', 'HMAC-SHA1', 'HMAC-MD5'] .
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
18	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 128.30.52.100 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.365078 Longitude: -71.104523 View: Google Map
creativecommons.org	ok	IP: 104.20.151.16 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
treehouses.media.mit.edu	ok	IP: 18.27.196.228 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.365078 Longitude: -71.104523 View: Google Map
mikepenz.com	ok	IP: 172.67.141.197 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
fontawesome.io	ok	IP: 54.198.239.119 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
gitter.im	ok	IP: 52.7.183.98 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	IP: 142.251.36.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
design.google.com	ok	IP: 142.251.39.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
schemas.android.com	ok	No Geolocation information available.
treehouses.io	ok	IP: 185.199.108.153 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
materialdesignicons.com	ok	IP: 34.234.179.93 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
scripts.sil.org	ok	IP: 104.22.11.254 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
octicons.github.com	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
xmlpull.org	ok	IP: 74.50.61.58 Country: United States of America Region: Texas City: Dallas Latitude: 32.814899 Longitude: -96.879204 View: Google Map

DOMAIN	STATUS	GEOLOCATION
fontawesome.com	ok	IP: 104.18.23.52 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.google.com	ok	IP: 142.250.179.164 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
this@terminalview.context	io/treehouses/remote/ssh/terminal/f.java
curve25519-sha256@libssh.org	com/trilead/ssh2/crypto/dh/GenericDhExchange.java

EMAIL	FILE
-------	------

curve25519-sha256@libssh.org	com/trilead/ssh2/crypto/dh/Curve25519Exchange.java
hmac-sha1-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com	com/trilead/ssh2/crypto/digest/HMAC.java
hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com	com/trilead/ssh2/crypto/digest/MACs.java
zlib@openssh.com	com/trilead/ssh2/compression/CompressionFactory.java
curve25519-sha256@libssh.org	e/d/a/s/b.java
auth-agent@openssh.com	e/d/a/o/d.java
auth-agent-req@openssh.com	e/d/a/q/a.java

HARDCODED SECRETS

POSSIBLE SECRETS
"button_key_ctrl" : "Ctrl"
"button_key_end" : "End"
"button_key_esc" : "Esc"

POSSIBLE SECRETS
"button_key_f1" : "F1"
"button_key_f10" : "F10"
"button_key_f11" : "F11"
"button_key_f12" : "F12"
"button_key_f2" : "F2"
"button_key_f3" : "F3"
"button_key_f4" : "F4"
"button_key_f5" : "F5"
"button_key_f6" : "F6"
"button_key_f7" : "F7"
"button_key_f8" : "F8"
"button_key_f9" : "F9"
"button_key_home" : "Home"
"button_key_pgdn" : "PgDn"
"button_key_pgup" : "PgUp"
"key_type_ed25519" : "Ed25519"

POSSIBLE SECRETS
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"
"library_FontAwesome_authorWebsite" : "https://materialdesignicons.com/"
"library_GoogleMaterialDesignIcons_authorWebsite" : "https://www.google.com/"
"library_Octicons_authorWebsite" : "https://github.com/"
"library_crossfadedrawerlayout_authorWebsite" : "http://mikepenz.com/"
"library_crossfader_authorWebsite" : "http://mikepenz.com/"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"library_itemanimators_authorWebsite" : "http://mikepenz.com/"
"library_materialdrawer_authorWebsite" : "http://mikepenz.com/"
"library_materialize_authorWebsite" : "http://mikepenz.com/"
"password" : "Password"

Report Generated by - MobSF v3.5.2 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).