MOBSF

ANDROID STATIC ANALYSIS REPORT

Home smart (1.19.2)

File Name:	Home_smart_base.apk
Package Name:	com.ikea.tradfri.lighting
Scan Date:	Aug. 25, 2022, 4:26 p.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	10	2	3	2

FILE INFORMATION

File Name: Home_smart_base.apk
Size: 70.02MB
MD5: df5d9a2d118544a0a747a0101c2a5df2
SHA1: c64ce0804c58f9f885d799870fb234e7880483ca
SHA256: bf6fc84586c717528fb882254dcd9d2c7afb864b223fdf2de1002e4964a9eebe

APP INFORMATION

App Name: Home smart
Package Name: com.ikea.tradfri.lighting
Main Activity: com.ikea.tradfri.lighting.startup.activity.SplashActivity
Target SDK: 31
Min SDK: 26
Max SDK:
Android Version Name: 1.19.2
Android Version Code: 2613

APP COMPONENTS

Activities: 14
Services: 8
Receivers: 2
Providers: 3
Exported Activities: 4
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=NL, ST=Delft, L=Delft, O=IKEA, OU=Inter IKEA BV, CN=Lovisa Eriksson
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-02-21 13:43:24+00:00
Valid To: 2067-02-09 13:43:24+00:00
Issuer: C=NL, ST=Delft, L=Delft, O=IKEA, OU=Inter IKEA BV, CN=Lovisa Eriksson
Serial Number: 0x1f729e30
Hash Algorithm: sha256
md5: 83eb1052480d65d5f4b7d1bac806bf13
sha1: b981bee80189ea28921350a4cb5f6457530a145b
sha256: dcee140567706d6c496615d6036036e6a33c61a66b0275877a08797dd55d1994
sha512: 5b5c47808891bcc39336aa147280c2b62761af13ca9a05c52fdf08a2d5cd0659fb632dc17ab44c1fdbb6ee1c87cabaa45b41b6a2bfe45bb366c8fedcc977e966
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b56ba1b2ae243d40892b75dbdb4a3a0c9753bb4e76ee3b7a964f38ffa5bafca1

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

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
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	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check SIM operator check ro.product.device check
	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.amazon.identity.auth.device.workflow.WorkflowActivity	Schemes: amzn://, Hosts: com.ikea.tradfri.lighting,
com.ikea.tradfri.lighting.startup.activity.SplashActivity	Schemes: ikea://, Hosts: tradfri, Path Prefixes: /,
com.auth0.android.provider.RedirectActivity	Schemes: demo://,
com.ikea.tradfri.lighting.home.activity.WelcomeActivity	Schemes: ihs://,

net.openid.appauth.RedirectUriReceiverActivity	Schemes: com.ikea.tradfri.lighting://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (com.amazon.identity.auth.device.workflow.WorkflowActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
2	Activity (com.auth0.android.provider.RedirectActivity) is not Protected. [android:exported=true]	high	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	Activity (com.ikea.tradfri.lighting.home.activity.WelcomeActivity) is not Protected. [android:exported=true]	high	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 (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	high	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	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

6	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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/m.java a2/o.java b0/b.java c/d.java c0/e.java c0/f.java c0/j.java c2/c.java d/c.java d/f.java e2/d.java e2/g.java f2/a.java gb/f.java j/e0.java j/k0.java j/n0.java j/q.java j/s.java j/z.java k0/a.java k0/h.java k0/n.java k0/s.java

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	k3/s.java l3/q.java lc/b.java mc/a.java o5/c.java org/eclipse/jetty/util/TypeUtil.java org/eclipse/jetty/util/Uptime.java org/eclipse/jetty/util/component/ContainerLifeCycle.java org/eclipse/jetty/util/log/AbstractLogger.java org/eclipse/jetty/util/log/JettyLogHandler.java org/eclipse/jetty/util/log/LoggerLog.java org/eclipse/jetty/util/log/Slf4jLog.java org/eclipse/jetty/util/log/StacklessLogging.java org/eclipse/jetty/util/log/StdErrLog.java org/eclipse/jetty/util/security/Password.java org/eclipse/jetty/util/security/UnixCrypt.java p0/c.java p3/a.java pd/a.java q/d.java q1/b.java q1/h.java q3/a.java r5/c.java s/g.java sa/d.java t1/b.java t1/c.java t5/a.java t5/b0.java t5/c.java t5/c0.java t5/e.java

t5/f0.java
t5/p.java
t5/r.java
t5/t.java
t5/x.java
u/e.java
u2/b.java
u2/c.java
u2/d.java
u2/h.java
u2/i.java
u2/j.java
u2/l.java
u2/o.java
u2/p.java
u2/r.java
u2/u.java
v/a.java
v/b.java
v1/a0.java
v1/e.java
v1/n.java
v1/q.java
v1/r.java
v1/u.java
v1/v.java
v1/y.java
v1/z.java
v2/e.java
v2/k.java
x1/b.java
x1/c.java
x1/d.java
x1/f.java
x1/g.java
x2/q.java
x4/f.java
x4/w.java
y1/a.java
y1/b.java
y1/c.java
y1/d.java

				y1/e.java y1/f.java y1/k.java y1/l.java y2/o.java z/b.java z/c.java z/e.java z1/a.java z1/b.java z1/f.java z1/g.java z1/m.java z1/q.java
2	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	cd/a.java cd/b.java dd/a.java org/eclipse/californium/core/network/MessageIdTracker.java org/eclipse/californium/core/network/stack/ReliabilityLayer.java org/eclipse/jetty/client/util/DigestAuthentication.java org/eclipse/jetty/websocket/client/masks/RandomMasker.java
3	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	org/eclipse/jetty/http/MultiPartFormInputStream.java org/eclipse/jetty/util/MultiPartInputStreamParser.java q5/c.java
4	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	h0/a.java o2/i.java o2/k.java o2/l.java o2/m.java o2/n.java y1/i.java

5	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/ikea/tradfri/lighting/ipso/IPSOObjects.java com/ikea/tradfri/lighting/shared/model/ConfigDetails.java com/ikea/tradfri/lighting/shared/sonos/SonosGroupDiscovery.java org/eclipse/jetty/client/HttpClientTransport.java org/eclipse/jetty/io/ClientConnectionFactory.java org/eclipse/jetty/io/ManagedSelector.java org/eclipse/jetty/io/ssl/SslClientConnectionFactory.java org/eclipse/jetty/util/component/Dumpable.java
6	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	eb/a.java org/eclipse/jetty/websocket/common/AcceptHash.java q5/b.java r5/c.java t5/p.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/ikea/tradfri/lighting/shared/sonos/JettyWebSocketHelper.java gb/i.java org/eclipse/jetty/util/ssl/SslContextFactory.java qd/v.java
8	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	f9/a.java g9/e.java wa/w.java
9	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	u4/e1.java

10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	oc/a.java org/eclipse/jetty/client/util/SPNEGOAuthentication.java org/eclipse/jetty/util/StringUtil.java
11	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	mc/a.java org/eclipse/jetty/util/security/Credential.java
12	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	eb/a.java y1/b.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	x4/p.java
14	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	z1/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		True info The shared object has NX bit set. This marks a	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack	None info The shared object does not	None info The shared object does not have RUNPATH	False warning The shared object does not have any fortified functions. Fortified functions provides buffer	True info Symbols are stripped.

1	lib/x86/libwolfssl.so	memory page non-executable making attacker injected shellcode non-executable.	buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	have run-time search path or RPATH set.	set.	overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	
2	lib/x86/libwolfssljni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.
3	lib/arm64-v8a/libwolfssl.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__read_chk', '__vsprintf_chk', '__memset_chk', '__strncat_chk', '__strncpy_chk']	True info Symbols are stripped.
		True info The shared object has NX bit set. This	True info This shared object has a stack canary value added to the stack so that it will be	None info The shared object	None info The shared object does not have	False warning The shared object does not have any fortified functions. Fortified	True info Symbols are stripped.

4	lib/arm64-v8a/libwolfssljni.so	marks a memory page non-executable making attacker injected shellcode non-executable.	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.	does not have run-time search path or RPATH set.	RUNPATH set.	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.	
5	lib/x86_64/libwolfssl.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strncpy_chk', '__read_chk', '__strlen_chk', '__strncat_chk', '__vsnprintf_chk', '__vsprintf_chk']	True info Symbols are stripped.
6	lib/x86_64/libwolfssljni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.
		True info The shared object has NX	True info This shared object has a stack canary value added to	None info The shared	None info The shared object does	False warning The shared object does not have any fortified	True info Symbols are stripped.

7	lib/armeabi-v7a/libwolfssl.so	bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	object does not have run-time search path or RPATH set.	not have RUNPATH set.	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.	
8	lib/armeabi-v7a/libwolfssljni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

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', 'location', 'camera'].
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.
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(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.

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_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
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.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
19	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.
20	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
21	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 142.251.209.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
privacypolicy.config.homesmart.ikea.net	ok	**IP:** 18.64.119.97 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
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
app.config.homesmart.ikea.net	ok	**IP:** 18.64.119.54 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

www.eclipse.org	ok	IP: 198.41.30.198 Country: Canada Region: Ontario City: Ottawa Latitude: 45.345139 Longitude: -75.765076 View: Google Map
api.sandbox.amazon.com	ok	IP: 54.239.28.194 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
developer.android.com	ok	IP: 172.217.16.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
meta.config.homesmart.ikea.net	ok	IP: 52.222.191.103 Country: Germany Region: Baden-Wurttemberg City: Hamberg Latitude: 48.819820 Longitude: 8.774490 View: Google Map
schemas.android.com	ok	No Geolocation information available.
tools.ietf.org	ok	IP: 50.223.129.194 Country: United States of America Region: Georgia City: Marietta Latitude: 33.952599 Longitude: -84.549927

		View: Google Map
play.google.com	ok	IP: 142.250.181.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebase.google.com	ok	IP: 172.217.16.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
apac.account.amazon.com	ok	IP: 52.94.210.96 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
api.amazon.com	ok	IP: 209.54.178.164 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
na.account.amazon.com	ok	IP: 52.46.157.10 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488

		View: Google Map
www.youtube.com	ok	IP: 142.250.181.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ww8.ikea.com	ok	IP: 104.102.42.203 Country: Germany Region: Hamburg City: Hamburg Latitude: 53.575321 Longitude: 10.015340 View: Google Map
api.amazon.co.jp	ok	IP: 54.240.251.149 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
app-de.onetrust.com	ok	IP: 104.18.41.98 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
eclipse.org	ok	IP: 198.41.30.198 Country: Canada Region: Ontario City: Ottawa Latitude: 45.345139

		Longitude: -75.765076 View: Google Map
webhook.logentries.com	ok	IP: 54.194.162.92 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
eu.account.amazon.com	ok	IP: 52.94.216.25 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
api.sandbox.amazon.co.uk	ok	IP: 54.239.35.49 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
api-sandbox.amazon.co.jp	ok	IP: 54.240.252.254 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
api.amazon.co.uk	ok	IP: 54.239.33.207 Country: Ireland Region: Dublin City: Dublin

		Latitude: 53.343990 **Longitude:** -6.267190 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.16.77 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ikea.com	ok	**IP:** 2.16.193.17 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **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
javax.xml.xmlconstants	ok	No Geolocation information available.
supportdetails.config.homesmart.ikea.net	ok	**IP:** 52.85.92.56 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Hamberg **Latitude:** 48.819820 **Longitude:** 8.774490 **View:** Google Map
		IP: 93.184.216.34

www.example.com	ok	**Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
plus.google.com	ok	**IP:** 142.251.209.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	v2/p.java

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyAN5LTxo0K0YFXKpOjoN8dKOE61UyIbA1c"
"google_crash_reporting_api_key" : "AIzaSyAN5LTxo0K0YFXKpOjoN8dKOE61UyIbA1c"

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.