ANDROID STATIC ANALYSIS REPORT

Home Assistant (3.0.0-minimal)

File Name:	installer136.apk
Package Name:	io.homeassistant.companion.android.minimal
Scan Date:	May 31, 2022, 1:27 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	21	1	2	2

FILE INFORMATION

File Name: installer136.apk
Size: 8.12MB
MD5: e60efc50752a38a6d49a137785ad1aef
SHA1: 15c6b26c1ca5403c5800fe55f63776bcda00278b
SHA256: c590de9f75924875cb938283c71321ecf2d086a030387696b3e481a2377db7fd

APP INFORMATION

App Name: Home Assistant
Package Name: io.homeassistant.companion.android.minimal
Main Activity: io.homeassistant.companion.android.launch.LaunchActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 3.0.0-minimal
Android Version Code: 504

APP COMPONENTS

Activities: 12
Services: 6
Receivers: 15
Providers: 2
Exported Activities: 7
Exported Services: 3
Exported Receivers: 8
Exported Providers: 0

✹ CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-13 12:10:56+00:00
Valid To: 2048-01-30 12:10:56+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x3a18186b9ab6ea7d
Hash Algorithm: sha256
md5: 79e3d3750e704e5e1b2f0ec638b1d555
sha1: d3377803da0148da2a41e5ab6ad62378dbcc2ec3
sha256: 17485250a03a0f2b3f292a054f595a9e794beef80cf910f7b3bbb8098abf6d50
sha512: 501cf88cb5c1217a7123cb7d0248693a6c0304c68e8e09b880fedf0c82eec99f0f622596a249d03b00bcc850567eaf456c8b13b6afc87a667b29c70bdd3986c8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c95430a391dfdab4cc5776a9b1c938565f650cbd65c095c0e9c102a177d38316

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACCESS_NOTIFICATION_POLICY	normal		Marker permission for applications that wish to access notification policy.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS

<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>Compiler</td><td>r8</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
io.homeassistant.companion.android.nfc.TagReaderActivity	Schemes: https://, Hosts: www.home-assistant.io, Path Prefixes: /tag/,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

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	Broadcast Receiver (io.homeassistant.companion.android.sensors.SensorReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (io.homeassistant.companion.android.widgets.button.ButtonWidget) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (io.homeassistant.companion.android.widgets.entity.EntityWidget) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (io.homeassistant.companion.android.widgets.media_player_controls.MediaPlayerControlsWidget) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (io.homeassistant.companion.android.widgets.template.TemplateWidget) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
8	Activity (io.homeassistant.companion.android.widgets.button.ButtonWidgetConfigureActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
9	Activity (io.homeassistant.companion.android.widgets.entity.EntityWidgetConfigureActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Activity (io.homeassistant.companion.android.widgets.media_player_controls.MediaPlayerControlsWidgetConfigureActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
11	Activity (io.homeassistant.companion.android.widgets.template.TemplateWidgetConfigureActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Service (io.homeassistant.companion.android.sensors.NotificationSensorManager) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Service (io.homeassistant.companion.android.controls.HaControlsProviderService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CONTROLS [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Broadcast Receiver (io.homeassistant.companion.android.sensors.LocationSensorManager) is not Protected. [android:exported=true]	high	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.
15	Broadcast Receiver (io.homeassistant.companion.android.sensors.ActivitySensorManager) is not Protected. [android:exported=true]	high	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.
16	Activity (io.homeassistant.companion.android.nfc.TagReaderActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Activity (io.homeassistant.companion.android.share.ShareActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
18	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
20	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/homeassistant/companion/android/widgets/button/ButtonWidget.java io/homeassistant/companion/android/webview/WebViewActivity$onActivityResult$1.java io/homeassistant/companion/android/settings/SettingsPresenterImpl$nfcEnabled$1.java io/homeassistant/companion/android/nfc/NfcViewModel.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$callRewindService$1.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidgetConfigureActivity.java io/homeassistant/companion/android/webview/WebViewActivity$onCreate$4$4$externalBus$1$1.java io/homeassistant/companion/android/settings/SettingsFragment.java io/homeassistant/companion/android/nfc/NfcSetupActivity.java io/homeassistant/companion/android/onboarding/discovery/HomeAssistantSearcher.java io/homeassistant/companion/android/sensors/TrafficStatsManager.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$saveEntityConfiguration$1.java io/homeassistant/companion/android/sensors/NetworkSensorManager.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$callFastForwardService$1.java io/homeassistant/companion/android/sensors/DNDSensorManager.java io/homeassistant/companion/android/controls/HaControlsProviderService$refresh$1$run$$inlined$forEach$lambda$1.java io/homeassistant/companion/android/nfc/NfcEditFragment.java io/homeassistant/companion/android/common/data/integration/impl/IntegrationRepositoryImpl.java io/homeassistant/companion/android/controls/HaControlsProviderService.java io/homeassistant/companion/android/widgets/template/TemplateWidget.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	io/homeassistant/companion/android/sensors/SensorReceiver.java eightbitlab/com/blurview/BlurView.java io/homeassistant/companion/android/sensors/LightSensorManager.java io/homeassistant/companion/android/launch/LaunchPresenterImpl$resyncRegistration$1.java io/homeassistant/companion/android/widgets/button/ButtonWidgetConfigureActivity.java io/homeassistant/companion/android/sensors/NextAlarmManager.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidgetConfigureActivity$onCreate$1.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$callPreviousTrackService$1.java io/homeassistant/companion/android/sensors/StepsSensorManager.java io/homeassistant/companion/android/database/AppDatabase$Companion$notifyMigrationFailed$2.java io/homeassistant/companion/android/widgets/entity/EntityWidget$saveEntityConfiguration$1.java io/homeassistant/companion/android/widgets/entity/EntityWidget.java io/homeassistant/companion/android/sensors/PressureSensorManager.java io/homeassistant/companion/android/settings/SettingsPresenterImpl$getNotificationRateLimits$1.java io/homeassistant/companion/android/share/ShareActivity$onCreate$3.java io/homeassistant/companion/android/sensors/StorageSensorManager.java io/homeassistant/companion/android/webview/WebViewPresenterImpl$onGetExternalAuth$1.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidgetConfigureActivity$onCreate$entity$1.java io/homeassistant/companion/android/webview/WebViewPresenterImpl$onViewReady$1.java io/homeassistant/companion/android/widgets/button/ButtonWidgetConfigureActivity$onCreate$1.java com/maltaisn/icondialog/pack/IconDrawableLoader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/homeassistant/companion/android/onboarding/integration/MobileAppIntegrationPresenterBase$onRegistrationAttempt$1.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$callPlayPauseService$1.java io/homeassistant/companion/android/widgets/button/ButtonWidget$saveServiceCallConfiguration$1.java io/homeassistant/companion/android/settings/SettingsPresenterImpl$putString$1.java io/homeassistant/companion/android/nfc/TagReaderActivity$onCreate$1.java io/homeassistant/companion/android/database/AppDatabase.java io/homeassistant/companion/android/sensors/SensorWorker$doWork$2.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget.java io/homeassistant/companion/android/controls/HaControlsProviderService$performControlAction$1.java io/homeassistant/companion/android/widgets/entity/EntityWidgetConfigureActivity$onCreate$entity$1.java io/homeassistant/companion/android/widgets/media_player_controls/MediaPlayerControlsWidget$callNextTrackService$1.java io/homeassistant/companion/android/onboarding/authentication/AuthenticationPresenterImpl$onViewReady$1.java io/homeassistant/companion/android/webview/WebViewActivity.java io/homeassistant/companion/android/widgets/entity/EntityWidgetConfigureActivity$onCreate$3.java io/homeassistant/companion/android/nfc/SingleLiveEvent.java io/homeassistant/companion/android/webview/WebViewPresenterImpl$onRevokeExternalAuth$1.java io/homeassistant/companion/android/sensors/ProximitySensorManager.java io/homeassistant/companion/android/onboarding/authentication/AuthenticationPresenterImpl$onRedirectUrl$1.java io/homeassistant/companion/android/widgets/button/ButtonWidget$callConfiguredService$1.java io/homeassistant/companion/android/widgets/entity/EntityWidgetConfigureActivity.java io/homeassistant/companion/android/webview/WebViewActivity$exoPlayHls$2.java io/homeassistant/companion/android/onboarding/manual/Manua

NO	ISSUE	SEVERITY	STANDARDS	FILES
				lSetupPresenterImpl$onClickOk$1.java io/homeassistant/companion/android/widgets/common/WidgetDynamicFieldAdapter.java io/homeassistant/companion/android/authenticator/Authenticator.java io/homeassistant/companion/android/sensors/LastUpdateManager.java
2	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.]()	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	io/homeassistant/companion/android/common/data/integration/impl/IntegrationRepositoryImpl.java io/homeassistant/companion/android/database/authentication/Authentication.java io/homeassistant/companion/android/common/data/integration/impl/entities/RegisterDeviceResponse.java io/homeassistant/companion/android/common/data/integration/impl/entities/DiscoveryInfoResponse.java
3	[App can read/write to External Storage. Any App can read data written to External Storage.]()	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	io/homeassistant/companion/android/sensors/StorageSensorManager.java
4	[This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.]()	secure	OWASP MASVS: MSTG-NETWORK-4	io/homeassistant/companion/android/common/data/HomeAssistantRetrofit.java

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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['NFC', 'network connectivity', 'bluetooth', 'location', 'camera', 'microphone'].
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_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.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	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.
14	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
eksempel.duckdns.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
pelda.com	ok	**IP:** 45.79.19.196 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **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
esempio.com	ok	**IP:** 195.110.124.188 **Country:** Italy **Region:** Toscana **City:** Florence **Latitude:** 43.766670 **Longitude:** 11.250000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
esimerkki.duckdns.org	ok	No Geolocation information available.
home-assistant.io	ok	**IP:** 104.26.5.238 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ornek.com	ok	**IP:** 172.67.208.64 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
alanadiniz.duckdns.org	ok	No Geolocation information available.
www.home-assistant.io	ok	**IP:** 104.26.5.238 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.ipify.org	ok	**IP:** 3.232.242.170 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pelda.duckdns.org	ok	**IP:** 192.168.1.140 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
exemple.duckdns.org	ok	**IP:** 34.125.248.99 **Country:** United States of America **Region:** Nevada **City:** Las Vegas **Latitude:** 36.174969 **Longitude:** -115.137222 **View:** Google Map
eksempel.com	ok	**IP:** 76.223.65.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
eksempel.no	ok	**IP:** 3.67.255.218 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
minuha.com	ok	No Geolocation information available.
ejemplo.duckdns.org	ok	**IP:** 179.6.47.57 **Country:** Peru **Region:** Lambayeque **City:** Chiclayo **Latitude:** -6.773610 **Longitude:** -79.841667 **View:** Google Map
mobile-apps.home-assistant.io	ok	**IP:** 151.101.1.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
esempio.duckdns.org	ok	**IP:** 185.198.166.18 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ipify.org	ok	**IP:** 64.185.233.11 **Country:** United States of America **Region:** Utah **City:** Ogden **Latitude:** 41.276379 **Longitude:** -111.987442 **View:** Google Map
example.duckdns.org	ok	**IP:** 84.249.67.149 **Country:** Finland **Region:** Varsinais-Suomi **City:** Turku **Latitude:** 60.451481 **Longitude:** 22.268690 **View:** Google Map
ipify.org来确定ip地址	ok	No Geolocation information available.
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
ejemplo.com	ok	**IP:** 216.120.146.201 **Country:** United States of America **Region:** Michigan **City:** Grandville **Latitude:** 42.898064 **Longitude:** -85.757111 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "firebase_url"
"google_api_key" : "current_key"
"google_crash_reporting_api_key" : "current_key"
"password" : "Password"
"username" : "Username"
"password" : "Contrasenya"
"password" : "Adgangskode"
"username" : "Brugernavn"
"password" : "Passwort"
"username" : "Benutzername"
"password" : "Salasana"
"username" : "Käyttäjätunnus"
"password" : "Heslo"
"password" : "Wachtwoord"

POSSIBLE SECRETS
"username" : "Gebruikersnaam"
"password" : "Hasło"
"password" : "Passord"
"username" : "Brukernavn"
"password" : "Parola"
"password" : "Heslo"
"password" : "Contraseña"
"password" : "Salasõna"
"username" : "Kasutajanimi"
"password" : "Password"
"password" : "Jelszó"
"username" : "Felhasználónév"
"password" : "Пароль"
"username" : "Логин"
"password" : "Parole"
"username" : "Lietotājvārds"

POSSIBLE SECRETS
"password" : "Lösenord"
"username" : "Användarnamn"
"password" : "Wachtwurd"
"username" : "Brûkersnamme"
"not_private" : "您与该站点的连接不是私有的。"
"password" : "密码"
"session_timeout_title" : "会话超时（秒）"
"username" : "用户名"
"password" : "비밀번호"
"password" : "密碼"
"username" : "使用者名稱"

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.