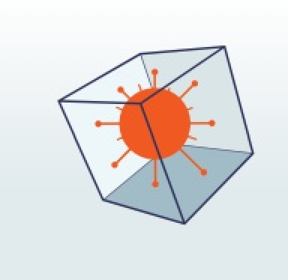
MobSF

ANDROID STATIC ANALYSIS REPORT



Smittestopp (3.2.1)

File Name:	Smittestopp_v3.2.1_apkpure.com.xapk
Package Name:	no.fhi.smittestopp_exposure_notification
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	2/421
Scan Date:	Feb. 20, 2022, 7:15 p.m.

FILE INFORMATION

File Name: Smittestopp_v3.2.1_apkpure.com.xapk
Size: 13.01MB
MD5: 6042ed7216712aa77fcb19a8b002bd25

SHA1: c371de0d9ae5386dc0426483dc7cf99153c1a5be
SHA256: bb244d329319ceda116c5b0542ea58c6687f924231989e8172099313289d8d31

APP INFORMATION

App Name: Smittestopp
Package Name: no.fhi.smittestopp_exposure_notification
Main Activity: crc64d475fe8a9f96ce4e.InitializerActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 3.2.1
Android Version Code: 44

APP COMPONENTS

Activities: 31
Services: 9
Receivers: 17
Providers: 3
Exported Activities: 1
Exported Services: 2
Exported Receivers: 6
Exported Providers: 0

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: 2020-11-10 14:23:38+00:00
Valid To: 2050-11-10 14:23:38+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4e4bb861684d6cb4af45ad109e4b7ec1cf8ac7ae
Hash Algorithm: sha256
md5: 24fc3853168fa625df687719f04a6ca9
sha1: a07d7ce0b3f3a27a83abb82cbec8cd25547dac7b
sha256: 2faa2a9e1c661e096836e6b0973ea9f4dacb5aed329fa13d6fb82d38c93be221
sha512: 301582d293e00d5d65100b32df864f169650d62de5e9d6ea520328c545af032f2404d25505253d632387b3f026deccbe3ee0afbd111def492bc2e478084abb4f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: bbaa66ac9e36d90c69f9874d636fbc1871b71519f5769cfc8423f342b08ba735

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
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.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.

PERMISSION	STATUS	INFO	DESCRIPTION
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.HARDWARE check network operator name check possible VM check
	Compiler	unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
md52ecc484fd43c6baf7f3301c3ba1d0d0c.AuthUrlSchemeInterceptorActivity	Schemes: no.fhi.smittestopp-exposure-notification://, Paths: /oauth2redirect,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (md52ecc484fd43c6baf7f3301c3ba1d0d0c.AuthUrlSchemeInterceptorActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
2	Broadcast Receiver (crc644071226567a85653.BluetoothStateBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (crc644071226567a85653.FlightModeHandlerBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (crc644071226567a85653.BackgroundNotificationBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
5	Broadcast Receiver (crc644071226567a85653.PermissionsBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (crc64f5fe2524876ceee4.ExposureNotificationCallbackBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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. 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
7	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]	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. 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.
8	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]	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. 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.
9	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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. 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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
mobile.events.data.microsoft.com	good	**IP:** 20.189.173.9 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
in.appcenter.ms	good	**IP:** 40.70.161.7 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

URLS

URL	FILE
https://in.appcenter.ms	com/microsoft/appcenter/ingestion/AppCenterIngestion.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	com/microsoft/appcenter/ingestion/OneCollectorIngestion.java

TRACKERS

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

PLAYSTORE INFORMATION

Title: Smittestopp

Score: 3.4285715 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** no.fhi.smittestopp_exposure_notification

Developer Details: Folkehelseinstituttet, Folkehelseinstituttet, None, https://www.fhi.no, folkehelseinstituttet@fhi.no,

Release Date: Dec 14, 2020 **Privacy Policy:** Privacy link

Description:

The use of Smittestopp is voluntary, and the app is one of many measures to limit the spread of coronavirus. You will receive a message if you have been nearby someone who has coronavirus. If you become infected, you can inform other app users. This way we can all take better care of those we surround us with. You cannot see who or how many people you have been in proximity to, and they cannot see you. If you share that you have been infected, other users cannot see your identity. The app does not register data about your location. Smittestopp is developed by the Norwegian Institute of Public Health. Read more about the app onwww.helsenorge.no/en/smittestopp If you experience a problem, that you believe the developers of the App should be aware of, you can report it as an issue on GitHub: https://github.com/folkehelseinstituttet/Fhi.Smittestopp.App/issues

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 v3.4.5 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.