




ANDROID STATIC ANALYSIS REPORT



 Calendar (2021.23.2-379299120-release)

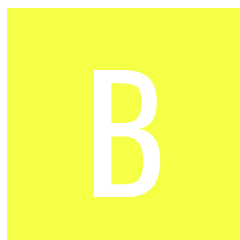
File Name: CalendarGooglePrebuilt.apk

Package Name: com.google.android.calendar

Scan Date: March 9, 2024, 6:44 a.m.






App Security Score: 49/100 (MEDIUM RISK)

Grade:



Trackers Detection: 1/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	46	2	1	1

FILE INFORMATION

File Name: CalendarGooglePrebuilt.apk

Size: 32.53MB

MD5: ec04c4dc56f053c9ed9789e345ae8378

SHA1: 633f87d807242ca3199a1fe6a681f4335d415144

SHA256: 20bd5ed0a4041152119ec42d39fdd7bca330e225c41c0877dba7b014baa78f0e

APP INFORMATION

App Name: Calendar

Package Name: com.google.android.calendar

Main Activity:

Target SDK: 30

Min SDK: 21

Max SDK:

Android Version Name: 2021.23.2-379299120-release

Android Version Code: 2017005112

APP COMPONENTS

Activities: 35

Services: 19

Receivers: 35

Providers: 5

Exported Activities: 9

Exported Services: 2

Exported Receivers: 22

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2008-08-21 23:13:34+00:00

Valid To: 2036-01-07 23:13:34+00:00

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

Serial Number: 0xc2e08746644a308d

Hash Algorithm: md5

md5: cde9f6208d672b54b1dacc0b7029f5eb

sha1: 38918a453d07199354f8b19af05ec6562ced5788

sha256: f0fd6c5b410f25cb25c3b53346c8972fae30f8ee7411df910480ad6b2d60db83

sha512: edf99db872937471eb94cbe576512a0089527e28b5b65df96f18f539737955ef1ce2553a51156ee31b521dcdc1559c52e965899f13038487d03743742b634326

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 843817f137559b510590075c0256a414a5767c6f32f91a46228077c065ba67fe

Found 1 unique certificates

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
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_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.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
com.google.android.googleapps.permission.GOOGLE_AUTH	unknown	Unknown permission	Unknown permission from android reference
android.permission.SUBSCRIBED_FEEDS_READ	normal	read subscribed feeds	Allows an application to receive details about the currently synced feeds.
android.permission.SUBSCRIBED_FEEDS_WRITE	dangerous	write subscribed feeds	Allows an application to modify your currently synced feeds. This could allow a malicious application to change your synced feeds.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.calendar.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gm.permission.READ_GMAIL	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gm.exchange.BIND	unknown	Unknown permission	Unknown permission from android reference
com.google.android.hangouts.START_HANGOUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.INTERACT_ACROSS_PROFILES	normal	enables interaction across profiles in the same group.	Allows interaction across profiles in the same profile group.
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.

FILE	DETAILS										
/home/mobsf/.MobSF/uploads/ec04c4dc56f053c9ed9789e345ae8378/ec04c4dc56f053c9ed9789e345ae8378.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr></table>	FINDINGS	DETAILS	Anti Disassembly Code	illegal class name						
FINDINGS	DETAILS										
Anti Disassembly Code	illegal class name										
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr><tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr></table>	FINDINGS	DETAILS	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check	Anti Debug Code	Debug.isDebuggerConnected() check	Compiler	r8 without marker (suspicious)	Anti Disassembly Code	illegal class name
FINDINGS	DETAILS										
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check										
Anti Debug Code	Debug.isDebuggerConnected() check										
Compiler	r8 without marker (suspicious)										
Anti Disassembly Code	illegal class name										

FILE	DETAILS						
classes2.dex	<table> <tr> <th>FINDINGS</th><th>DETAILS</th></tr> <tr> <td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check</td></tr> <tr> <td>Compiler</td><td>r8 without marker (suspicious)</td></tr> </table>	FINDINGS	DETAILS	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check	Compiler	r8 without marker (suspicious)
FINDINGS	DETAILS						
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check						
Compiler	r8 without marker (suspicious)						
classes3.dex	<table> <tr> <th>FINDINGS</th><th>DETAILS</th></tr> <tr> <td>Compiler</td><td>r8 without marker (suspicious)</td></tr> </table>	FINDINGS	DETAILS	Compiler	r8 without marker (suspicious)		
FINDINGS	DETAILS						
Compiler	r8 without marker (suspicious)						

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.android.calendar.event.LaunchInfoActivity	Schemes: http://, https://, Hosts: www.google.com, calendar.google.com, Mime Types: vnd.android.cursor.item/event, vnd.android.cursor.dir/event, Path Prefixes: /calendar/event, /calendar/mevent, /calendar/render, Path Patterns: /calendar, /calendar/, /calendar/hosted.*/event, /calendar/hosted.*/render, /,

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 37 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
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	TaskAffinity is set for activity (com.google.android.calendar.event.EventInfoActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
4	TaskAffinity is set for activity (com.android.calendar.event.LaunchInfoActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
5	Activity (com.android.calendar.event.LaunchInfoActivity) is not Protected. [android:exported=true]	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.
6	Activity-Alias (com.android.calendar.AllInOneActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias 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
7	Activity-Alias (com.android.calendar.LaunchActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity-Alias (com.google.android.calendar.timely.settings.CalendarPublicPreferenceActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity-Alias (com.google.android.calendar.ICallLauncher) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.google.android.calendar.AlternateSearchActivity) 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
11	Broadcast Receiver (com.google.android.calendar.timely.report.DebugCleanupReceiver) is not Protected. [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.
12	Service (com.google.android.calendar.timely.CalendarOobeService) is Protected by a permission. Permission: com.google.android.calendar.permission.READ_OOBE protectionLevel: signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.
13	Broadcast Receiver (com.google.android.calendar.SyncUpgradeReceiver) is not Protected. [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.
14	Broadcast Receiver (com.google.android.calendar.AllPrefsUpgradeReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Broadcast Receiver (com.google.android.apps.calendar.sync.SyncOnUnlockReceiver) is not Protected. [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.
16	Broadcast Receiver (com.google.android.apps.calendar.removeaccountdata.AccountDataCleaner) is not Protected. [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.
17	Broadcast Receiver (com.android.calendar.widget.CalendarAppWidgetProvider) is not Protected. [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.
18	Service (com.google.android.calendar.alerts.RemindersListenerService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Activity (com.google.android.calendar.PrivacyPolicyActivity) is not Protected. [android:exported=true]	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.
20	Service (com.google.android.syncadapters.calendar.CalendarSyncAdapterService) is not Protected. [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.
21	Broadcast Receiver (com.google.calendar.v2a.shared.sync.impl.android.accounts.AccountsBroadcastReceiver) is not Protected. [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.
22	Broadcast Receiver (com.google.android.calendar.widgetmonth.MonthViewWidgetProvider) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Broadcast Receiver (com.google.android.calendar.widgetmonth.MonthViewWidgetModelRefresher) is not Protected. [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.
24	Broadcast Receiver (com.google.android.syncadapters.calendar.ObsoleteDataCleanerBroadcastReceiver) is not Protected. [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.
25	TaskAffinity is set for activity (com.google.android.calendar.event.CrossProfileEventInfoActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
26	Broadcast Receiver (com.google.android.apps.calendar.config.phenotypesupport.broadcast.PhenotypeBroadcastReceiver) is not Protected. [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.
27	Broadcast Receiver (com.google.android.apps.calendar.usernotifications.NotificationsInitializer\$NotificationsRelevantUpdatesReceiver) is not Protected. [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.
28	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.inject.GrowthKitBootCompletedBroadcastReceiver) is not Protected. [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.
29	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.internal.debug.TestingToolsBroadcastReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Broadcast Receiver (com.google.android.libraries.internal.growth.growthkit.internal.experiments.impl.PhenotypeBroadcastReceiver) is not Protected. [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.
31	Broadcast Receiver (com.google.android.libraries.notifications.entrpoints.accountchanged.AccountChangedReceiver) is not Protected. [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.
32	Broadcast Receiver (com.google.android.libraries.notifications.entrpoints.blockstatechanged.BlockStateChangedReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
33	<p>Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.gcm.GcmBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
34	<p>Broadcast Receiver (com.google.android.libraries.notifications.entrypoints.phenotype.PhenotypeUpdateReceiver) is not Protected.</p> <p>[android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
35	Broadcast Receiver (com.google.android.libraries.notifications.entrpoints.restart.RestartReceiver) is not Protected. [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.
36	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.AccountRemovedBroadcastReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
37	<p>Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeUpdateBackgroundBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [android:exported=true]</p>	warning	<p>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.</p>
38	<p>Activity (com.google.android.libraries.social.licenses.LicenseMenuActivity) is not Protected. [android:exported=true]</p>	warning	<p>An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
39	Activity (com.google.android.libraries.surveys.internal.view.SurveyActivity) is not Protected. [android:exported=true]	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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/C0004if.java cal/aae.java cal/aax.java cal/abae.java cal/abao.java cal/abas.java cal/abns.java cal/abpi.java cal/abpo.java cal/abpv.java cal/abqv.java cal/acb.java cal/ado.java cal/afd.java cal/aff.java cal/agsw.java cal/aguv.java cal/akr.java cal/akv.java cal/akz.java cal/ame.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/aou.java cal/api.java cal/apr.java cal/atn.java cal/aug.java cal/auj.java cal/aup.java cal/av.java cal/awb.java cal/awh.java cal/awi.java cal/awj.java cal/awl.java cal/awn.java cal/awq.java cal/axi.java cal/axn.java cal/axx.java cal/ayj.java cal/ayz.java cal/azj.java cal/azk.java cal/bfq.java cal/bgd.java cal/bgp.java cal/biu.java cal/bla.java cal/ble.java cal/bnn.java cal/boc.java cal/boj.java cal/bqd.java cal/brs.java cal/bry.java cal/bsd.java cal/bsq.java cal/bsr.java cal/bsu.java cal/btc.java cal/bus.java cal/bwz.java cal/bwz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/bxi.java cal/csz.java cal/ceq.java cal/cer.java cal/cma.java cal/cry.java cal/drt.java cal/dtt.java cal/duj.java cal/dup.java cal/dvg.java cal/dxh.java cal/dzp.java cal/eeq.java cal/ejt.java cal/eju.java cal/ejv.java cal/elh.java cal/erj.java cal/erk.java cal/esq.java cal/gl.java cal/gom.java cal/gy.java cal/gyx.java cal/hky.java cal/ho.java cal/hp.java cal/ik.java cal/io.java cal/iom.java cal/ip.java cal/iq.java cal/iw.java cal/ix.java cal/jd.java cal/jr.java cal/kes.java cal/kfe.java cal/kgr.java cal/ki.java cal/kis.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	cal/kj.java cal/ko.java cal/ktf.java cal/ldh.java cal/ldj.java cal/li.java cal/lk.java cal/lob.java cal/lq.java cal/lw.java cal/lxs.java cal/mjm.java cal/mnt.java cal/msm.java cal/oak.java cal/odw.java cal/ofc.java cal/ooz.java cal/orb.java cal/oru.java cal/otr.java cal/ouj.java cal/oxe.java cal/pd.java cal/pfa.java cal/pfw.java cal/pgc.java cal/pgd.java cal/pgh.java cal/pgv.java cal/phb.java cal/phm.java cal/phr.java cal/pit.java cal/pjj.java cal/plo.java cal/plp.java cal/plq.java cal/pmn.java cal/ppt.java cal/ptf.java cal/ptg.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/ptv.java cal/puf.java cal/pub.java cal/puf.java cal/puv.java cal/pvb.java cal/pwn.java cal/pxm.java cal/pyt.java cal/pyx.java cal/pze.java cal/pzf.java cal/pzs.java cal/pzw.java cal/qca.java cal/qes.java cal/qex.java cal/qfc.java cal/qfj.java cal/qfk.java cal/qgu.java cal/qgv.java cal/qhr.java cal/qic.java cal/qrp.java cal/qrw.java cal/qty.java cal/qux.java cal/qwz.java cal/qyv.java cal/rgn.java cal/rim.java cal/rji.java cal/rjn.java cal/rlp.java cal/rlx.java cal/rmm.java cal/rp.java cal/rpy.java cal/rq.java cal/rqj.java cal/rnk.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/rqf.java cal/rrf.java cal/rth.java cal/sbw.java cal/sdd.java cal/sdt.java cal/sn.java cal/spp.java cal/sqq.java cal/swk.java cal/sxj.java cal/tbu.java cal/tby.java cal/tbz.java cal/ttq.java cal/tts.java cal/ttt.java cal/tue.java cal/tuf.java cal/tug.java cal/tuh.java cal/tuj.java cal/twz.java cal/tyw.java cal/tzf.java cal/tzk.java cal/uaa.java cal/uhp.java cal/uu.java cal/uxq.java cal/vds.java cal/vdt.java cal/vq.java cal/vqw.java cal/vre.java cal/vrk.java cal/wap.java cal/wav.java cal/wbq.java cal/wca.java cal/wcr.java cal/wdb.java .. .

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cal/wn.java cal/wlw.java cal/wle.java cal/wok.java cal/wqv.java cal/wrf.java cal/wss.java cal/wvd.java cal/wvk.java cal/wvl.java cal/wvo.java cal/wvp.java cal/wvr.java cal/wvz.java cal/wwa.java cal/wwj.java cal/wwo.java cal/wwt.java cal/wwx.java cal/wxd.java cal/wxe.java cal/wxw.java cal/wyg.java cal/wzd.java cal/wzm.java cal/wzw.java cal/xaa.java cal/xaf.java cal/xbc.java cal/xck.java cal/xp.java cal/ywy.java cal/ywz.java cal/zf.java cal/zi.java cal/zj.java cal/zl.java cal/zo.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	cal/vrr.java
3	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	cal/abms.java cal/ppt.java cal/vxz.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	cal/aps.java cal/bsq.java cal/bsr.java cal/dup.java cal/dxk.java cal/smc.java cal/smg.java cal/smj.java cal/smp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	cal/abn.java cal/acb.java cal/afra.java cal/afwm.java cal/brh.java cal/eer.java cal/rjj.java cal/tew.java cal/trn.java cal/trq.java cal/trr.java cal/trs.java cal/tsb.java cal/tse.java cal/tsg.java cal/ueb.java cal/ypb.java cal/zlc.java cal/zli.java cal/zpf.java j\$/util/concurrent/ThreadLo calRandom.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	cal/ablk.java cal/aeub.java cal/axh.java cal/rlx.java cal/sxg.java
7	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	cal/krn.java cal/rgo.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	cal/anr.java cal/nlj.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cal/tts.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

🔗 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/24	android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	4/45	android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.CALL_PHONE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
--------	----------------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	IP: 172.217.194.95 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.
www.ccil.org	ok	IP: 74.125.130.121 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
dev-notifications-pa.corp.googleapis.com	ok	IP: 172.253.118.129 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
lh3.googleusercontent.com	ok	IP: 172.217.194.132 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
scone-pa.googleapis.com	ok	IP: 142.251.12.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	IP: 172.253.118.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ssl.gstatic.com	ok	IP: 172.217.194.94 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
autopush-proddata-notifications-pa.sandbox.googleapis.com	ok	IP: 74.125.24.81 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
play.google.com	ok	IP: 74.125.24.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.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
www.google.com	ok	IP: 74.125.68.147 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
tracedepot-pa.googleapis.com	ok	IP: 172.253.118.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
maps.googleapis.com	ok	IP: 74.125.68.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
notifications-pa.googleapis.com	ok	IP: 74.125.24.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
autopush-notifications-pa.sandbox.googleapis.com	ok	IP: 142.251.175.81 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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
staging-notifications-pa.sandbox.googleapis.com	ok	IP: 64.233.170.81 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
calendar.google.com	ok	IP: 142.250.4.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
one.google.com	ok	IP: 142.251.175.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.google-analytics.com	ok	IP: 142.251.175.113 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
support.google.com	ok	IP: 142.251.175.101 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

EMAIL	FILE
aac5lfd6263ulfh4tql8@group.calendar	cal/crz.java
u0013android@android.com0 u0013android@android.com	cal/pzr.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

HARDCODED SECRETS

POSSIBLE SECRETS
"conference_authorize_button" : "AUTHORIZE"
"id_key_birthday" : "birthday"
"id_key_cross_profile" : "cross_profile"
"id_key_general" : "general"
"id_key_holiday" : "holiday"
"id_key_smart_mail" : "smart_mail"

POSSIBLE SECRETS
"visibility_private" : "პირადი"
"visibility_private" : "■■■■■"
"conference_authorize_button" : "■■■■■■■■■"
"visibility_private" : "■■■■■■■■■■■"
"conference_authorize_button" : "GODKJENN"
"visibility_private" : "Privat"
"conference_authorize_button" : "АЎТАРЫЗАБАЦЬ"
"visibility_private" : "Приватная"
"conference_authorize_button" : "AUTORISIEREN"
"visibility_private" : "Vertraulich"
"visibility_private" : "■■■■■"
"visibility_private" : "■■■■■■■■■■■"
"conference_authorize_button" : "MAGTIG"
"visibility_private" : "Privaat"
"conference_authorize_button" : "УПЪЛНОМОЩАВАНЕ"
"visibility_private" : "Частно"

POSSIBLE SECRETS

```
"conference_authorization_required": "████████████████████"
```

```
"conference_authorize_button": "■■■■■"
```

```
"goal_session_deferred": "████████████████████"
```

```
"groove_schedule_sessions": "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
```

```
"task_assigned_to_user": "████████████████████"
```

```
"visibility_private": "██████"
```

```
"visibility_secret" : "████████"
```

```
"conference_authorize_button" : "HYVÄKSY"
```

```
"visibility_private" : "Yksityinen"
```

```
"visibility_private": "██████"
```

```
"visibility_private": "██████████"
```

```
"visibility_private": "Жеке"
```

```
"conference_authorize_button": "ОДОБРИ"
```

"visibility_private": "Приватен"

```
"conference_authorize_button": "AUTORIZOVAŤ"
```

"visibility_private" : "Súkromné"

POSSIBLE SECRETS
"conference_authorize_button" : "АВТОРИЗУВАТИ"
"visibility_private" : "Приватно"
"conference_authorize_button" : "ΕΞΟΥΣΙΟΔΟΤΗΣΗ"
"visibility_private" : "Ιδιωτικό"
"conference_authorize_button" : "AUTORIZAR"
"visibility_private" : "Privado"
"visibility_private" : "■■■■■■■■■■"
"conference_authorize_button" : "MACHTIGEN"
"visibility_private" : "Privé"
"conference_authorize_button" : "AUTORYZUJ"
"visibility_private" : "Prywatne"
"conference_authorize_button" : "ODOBRI"
"visibility_private" : "Zasebno"
"conference_authorize_button" : "PAHINTULUTAN"
"visibility_private" : "Pribado"
"visibility_private" : "□□□"

POSSIBLE SECRETS

```
"conference_authorization_required": "██████████████████████████████████████████"
```

```
"conference_authorize_button": "████████████████████"
```

[illegible]

```
"groove_schedule_sessions": "██████████████████████████████████████"
```

```
"task_assigned_to_user": "████████████████████"
```

```
"visibility_private": "████"
```

```
"visibility_secret": "████████████████"
```

```
"visibility_private": "██████████"
```

```
"conference_authorize_button" : "IZINKAN"
```

```
"visibility_private" : "Pribadi"
```

```
"conference_authorize_button" : "■■■■■■■■■■"
```

```
"visibility_private": "██████"
```

```
"conference_authorize_button": "3ΘBШΘΘΡΘX"
```

"visibility_private" : "Хувийн"

```
"conference_authorize_button" : ""
```

```
"visibility_private": "000"
```

POSSIBLE SECRETS
"visibility_secret" : "□□"
"conference_authorization_required" : "ໄຕ້ອງການການອະນຸມັດ"
"conference_authorize_button" : "ໃຫ້ການອະນຸຍາດ"
"goal_session_deferred" : "ກຳລັງຊອກຫາເວລາອື່ນ..."
"groove_schedule_sessions" : "ກຳນົດເຊດຊັນເປົ້າໝາຍ"
"task_assigned_to_user" : "ມອບໝາຍໃຫ້ທ່ານ"
"visibility_private" : "ສ່ວນຕົວ"
"visibility_secret" : "ສະເພາະແຕ່ຂ້ອຍ"
"conference_authorize_button" : "AUTORIZAȚI"
"visibility_private" : "Privat"
"conference_authorize_button" : "AUTORIZO"
"visibility_private" : "Privat"
"conference_authorize_button" : "تفويض"
"visibility_private" : "خاص"
"conference_authorize_button" : "AUTORISER"
"visibility_private" : "Privé"

POSSIBLE SECRETS
"conference_authorize_button" : "AUTORIZIRAJ"
"visibility_private" : "Osobno"
"visibility_private" : "■■■■■"
"visibility_private" : "■■■■■■■"
"visibility_private" : "Приватно"
"visibility_private" : "Privatno"
"conference_authorize_button" : "YETKİLENDİR"
"visibility_private" : "Gizli"
"visibility_private" : "نجى"
"visibility_private" : "■■■■■■■■■"
"conference_authorize_button" : "ODOBRI"
"visibility_private" : "Privatno"
"conference_authorize_button" : "SCHVÁLIT"
"visibility_private" : "Soukromá"
"conference_authorize_button" : "AUTORIZAR"
"visibility_private" : "Privado"

POSSIBLE SECRETS
"conference_authorize_button" : "LEYFA"
"visibility_private" : "Einkamál"
"conference_authorize_button" : "IZINKAN"
"visibility_private" : "Tertutup"
"conference_authorize_button" : "VOLITA"
"visibility_private" : "Privaatne"
"conference_authorize_button" : "AUTORIZZA"
"visibility_private" : "Privato"
"visibility_private" : "Privatus"
"visibility_private" : "Pribatua"
"visibility_private" : "■■■■■"
"conference_authorize_button" : "ENGEDÉLYEZÉS"
"visibility_private" : "Privát"
"conference_authorize_button" : "АВТОРИЗОВАТЬ"
"visibility_private" : "Личное"
"conference_authorize_button" : "GUNYAZA"

POSSIBLE SECRETS

```
"visibility_private": "Ubumfihlo"
```

```
"conference_authorize_button" : "AUTORIZĚT"
```

```
"visibility_private" : "Privāts"
```

```
"conference_authorize_button" : "AUKTORISERA"
```

```
"visibility_private" : "Privat"
```

```
"conference_authorize_button": "אישור"
```

"visibility_private" : "פרטי"

```
"conference_authorize_button": "IDHINISHA"
```

```
"conference_authorize_button" : "ԹՈՒՅԼՍՐԵԼ"
```

"visibility_private" : "Անձնական"

"visibility_private" : "Купуя"

```
"conference_authorize_button": "■ □ ■ ■ □ ■ ■ ■ □"
```

```
"visibility_private": "██████□██████"
```

```
"conference_authorize_button" : "DOĞRULAYIN"
```

```
"visibility_private" : "Şəxsi"
```

```
"conference_authorize_button" : "AVTORIZATSIYA"
```


POSSIBLE SECRETS
"visibility_private" : "Shaxsiy"
"conference_authorize_button" : "AUTORISER"
"visibility_private" : "Privé"
"conference_authorize_button" : "AUTHORISE"
"visibility_private" : "Private"
"conference_authorization_required" : "□□□□"
"conference_authorize_button" : "□□"
"goal_session_deferred" : "□□□□□□□□..."
"goal_session_deferred_offline" : "□□□□□□□□□□□□□□□□□□"
"groove_schedule_sessions" : "□□□□□□"
"task_assigned_to_user" : "□□□□□"
"visibility_private" : "□□□"
"visibility_secret" : "□□□□□"
"conference_authorization_required" : "□□□□"
"conference_authorize_button" : "□□"
"goal_session_deferred" : "□□□□□□□□..."

POSSIBLE SECRETS
"goal_session_deferred_offline" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"
"groove_schedule_sessions" : "XXXXXX"
"task_assigned_to_user" : "XXXXX"
"visibility_private" : "XXX"
"visibility_secret" : "XXXXX"
"conference_authorize_button" : "AUTHORISE"
"visibility_private" : "Private"
"conference_authorize_button" : "AUTORIZAR"
"visibility_private" : "Particular"
"conference_authorize_button" : "AUTORIZAR"
"visibility_private" : "Privado"
"conference_authorize_button" : "AUTORIZAR"
"visibility_private" : "Privado"
"conference_authorization_required" : "XXXXX"
"conference_authorize_button" : "XX"
"goal_session_deferred" : "XXXXXXXXXX..."

for more: Twitter: <https://twitter.com/googleworkspace> LinkedIn: <https://www.linkedin.com/showcase/googleworkspace> Facebook: <https://www.facebook.com/googleworkspace/>

Report Generated by - MobSF v3.9.4 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.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).