MOBSF

ANDROID STATIC ANALYSIS REPORT

Calculator (8.4.1 (520193683))

File Name:	com.google.android.calculator.apk
Package Name:	com.google.android.calculator
Scan Date:	July 8, 2023, 8:53 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	12	1	1	1

FILE INFORMATION

File Name: com.google.android.calculator.apk
Size: 3.23MB
MD5: 36c666e44d7e4d30d021444bfb90bb40
SHA1: c981051da2a21bde498f1f19a8209f0ec775d9a1
SHA256: 2871f00f9eb8bafe0d236b1f72299b8bae79902c036380ff5c1b7ae772238ccc

APP INFORMATION

App Name: Calculator
Package Name: com.google.android.calculator
Main Activity: com.android.calculator2.Calculator
Target SDK: 33
Min SDK: 23
Max SDK:
Android Version Name: 8.4.1 (520193683)

Android Version Code: 84100198

APP COMPONENTS

Activities: 3
Services: 6
Receivers: 4
Providers: 0
Exported Activities: 1
Exported Services: 1
Exported Receivers: 2
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=calculator_google
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-02 01:55:31+00:00
Valid To: 2042-09-17 01:55:31+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=calculator_google
Serial Number: 0x9a331067233c23ed
Hash Algorithm: sha1
md5: b9620ff646b8fa4b575bce9937d188b8
sha1: af24b7f3eff9d97ae6d8a84664e0e98888636110
sha256: 90e8b84c91ae47530018af7fc35a943716fc8d2271f03548a1833be0166e2066
sha512: 825ea8a93d3e8fa25ce3ff724ced856a623ae1195b70af803a62553bc8c4e206f8e71c565088b170cffee99c48d125390c8f6112b0ea6494c24bdf41dcf5c84d
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 31e5ab837cbeaeeb08573e019f8af72f9c30228a7d21c584d60cecb1edcb65f4

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.calculator.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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 Disassembly Code</td><td>illegal class name</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | 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 might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=23]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.

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	Service (com.android.calculator2.CalculatorTileService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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
4	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]	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

HIGH: **0** | WARNING: **5** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/aak.java defpackage/aar.java defpackage/aas.java defpackage/aca.java defpackage/acd.java defpackage/aco.java defpackage/adk.java defpackage/adp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ae.java defpackage/air.java defpackage/aix.java defpackage/ajg.java defpackage/ajm.java defpackage/akb.java defpackage/alb.java defpackage/alg.java defpackage/aly.java defpackage/ama.java defpackage/amb.java defpackage/amc.java defpackage/amf.java defpackage/amm.java defpackage/ao.java defpackage/ap.java defpackage/aq.java defpackage/aqa.java defpackage/aqo.java defpackage/aqp.java defpackage/aqy.java defpackage/ar.java defpackage/arb.java defpackage/arf.java defpackage/arg.java defpackage/arr.java defpackage/asd.java defpackage/asq.java defpackage/asx.java defpackage/ata.java defpackage/atn.java defpackage/atv.java defpackage/aua.java defpackage/auc.java defpackage/auf.java defpackage/auk.java defpackage/aul.java defpackage/aur.java defpackage/aus.java defpackage/aux.java defpackage/auz.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	defpackage/avu.java defpackage/awf.java defpackage/awp.java defpackage/awu.java defpackage/awy.java defpackage/axl.java defpackage/axu.java defpackage/ayf.java defpackage/ayq.java defpackage/azm.java defpackage/baz.java defpackage/bbj.java defpackage/bbw.java defpackage/bby.java defpackage/bdp.java defpackage/ben.java defpackage/bes.java defpackage/bib.java defpackage/bid.java defpackage/big.java defpackage/blc.java defpackage/bld.java defpackage/blx.java defpackage/bo.java defpackage/bpt.java defpackage/bqo.java defpackage/brp.java defpackage/bs.java defpackage/bup.java defpackage/buw.java defpackage/bvc.java defpackage/bvd.java defpackage/bvl.java defpackage/bvm.java defpackage/bvn.java defpackage/bvp.java defpackage/bvs.java defpackage/bwh.java defpackage/bwi.java defpackage/bwj.java defpackage/bws.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/bwv.java defpackage/bx.java defpackage/bzh.java defpackage/cah.java defpackage/cck.java defpackage/cct.java defpackage/cff.java defpackage/cgb.java defpackage/cip.java defpackage/cli.java defpackage/clq.java defpackage/clu.java defpackage/co.java defpackage/cp.java defpackage/df.java defpackage/ea.java defpackage/fp.java defpackage/fq.java defpackage/gk.java defpackage/iu.java defpackage/je.java defpackage/jm.java defpackage/jn.java defpackage/jr.java defpackage/jw.java defpackage/lg.java defpackage/lk.java defpackage/mi.java defpackage/ml.java defpackage/mm.java defpackage/mw.java defpackage/nm.java defpackage/o.java defpackage/ol.java defpackage/qm.java defpackage/qv.java defpackage/rf.java defpackage/ri.java defpackage/so.java defpackage/td.java defpackage/tq.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/tq.java defpackage/ud.java defpackage/uf.java defpackage/ug.java defpackage/ui.java defpackage/ul.java defpackage/un.java defpackage/uo.java defpackage/up.java defpackage/uu.java defpackage/uy.java defpackage/vb.java defpackage/vd.java defpackage/vh.java defpackage/vk.java defpackage/vn.java defpackage/vs.java defpackage/vt.java defpackage/vz.java defpackage/wt.java defpackage/wy.java defpackage/wz.java defpackage/xx.java defpackage/ys.java defpackage/yt.java defpackage/yu.java defpackage/yv.java defpackage/yw.java defpackage/zb.java defpackage/zc.java defpackage/zg.java defpackage/zh.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	defpackage/aly.java defpackage/bes.java defpackage/blp.java defpackage/bmd.java defpackage/bno.java defpackage/bpb.java defpackage/bti.java defpackage/btl.java defpackage/btt.java defpackage/btv.java defpackage/btw.java defpackage/cfb.java defpackage/cfy.java defpackage/cfz.java defpackage/cga.java defpackage/cqg.java defpackage/ded.java defpackage/dee.java defpackage/def.java defpackage/dej.java j$/util/concurrent/ThreadLocalRandom.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	defpackage/bes.java defpackage/cqe.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	defpackage/acq.java defpackage/ama.java defpackage/amd.java defpackage/azw.java defpackage/baj.java defpackage/bbd.java defpackage/beh.java defpackage/ben.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/bvd.java
6	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	defpackage/awy.java
7	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	defpackage/bxm.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.
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 ['network connectivity'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 does not encrypt files 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_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.
12	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
13	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.
14	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.

! 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.googleadservices.com	ok	**IP:** 198.18.0.48 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 198.18.0.47 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
plus.google.com	ok	**IP:** 198.18.0.50 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
calculator-app-eng.firebaseio.com	ok	**IP:** 198.18.0.45 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
google.com	ok	**IP:** 198.18.0.17 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 198.18.0.34 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
schemas.android.com	ok	**IP:** 198.18.0.52 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 198.18.0.53 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
app-measurement.com	ok	**IP:** 198.18.0.49 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 198.18.0.51 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://calculator-app-eng.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	defpackage/aqu.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://calculator-app-eng.firebaseio.com"

PLAYSTORE INFORMATION

Title: Calculator

Score: 4.41485 **Installs:** 1,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.google.android.calculator

Developer Details: Google LLC, 5700313618786177705, 1600 Amphitheatre Parkway, Mountain View 94043, http://www.google.com/, android-calculator-feedback@google.com,

Release Date: Mar 30, 2016 **Privacy Policy:** Privacy link

Description:

Calculator provides simple and advanced mathematical functions in a beautifully designed app. • Perform basic calculations such as addition, subtraction, multiplication, and division • Do scientific operations such as trigonometric, logarithmic, and exponential functions

---