MOBSF

ANDROID STATIC ANALYSIS REPORT

Vibrator Strong (5.2.10)

File Name:	com.tomsmucenieks.asimplevibrator_46.apk
Package Name:	com.tomsmucenieks.asimplevibrator
Scan Date:	Sept. 1, 2025, 10:32 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	15	3	0	1

FILE INFORMATION

File Name: com.tomsmucenieks.asimplevibrator_46.apk
Size: 25.53MB
MD5: 425c3d2bcfb5ed4b3ad426ec7fe0506d
SHA1: a21c68af2c87d1ab575c8e9507dc71e91eab45f6
SHA256: 2f8e5bdf4fc786be3c61407d272fe2d8a554908800d6cc53dfa4da39d05807f2

APP INFORMATION

App Name: Vibrator Strong
Package Name: com.tomsmucenieks.asimplevibrator
Main Activity:
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 5.2.10

Android Version Code: 46

APP COMPONENTS

Activities: 11
Services: 12
Receivers: 11
Providers: 4
Exported Activities: 6
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=LV, L=Riga, CN=Toms Mucenieks
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-09-25 19:45:25+00:00
Valid To: 2041-09-19 19:45:25+00:00
Issuer: C=LV, L=Riga, CN=Toms Mucenieks
Serial Number: 0x7ecc308f
Hash Algorithm: sha256
md5: 7cac04e523f5ac55aa30e1b5aa46a7a0
sha1: dfad309aa89ae7e1efcfc18f28dec9db1c1a9d3a
sha256: c0e379cca4f9ae7dda272c0227b9ca2c7149dbbdeec95c394f015d1c6afb0eba
sha512: 0e99187bc8aeda6ba2b5017932437e4f532b7c4f2567b63bacf0c73aa6780ee8166e506fc8b8d46f7b698aa1bead30cf1e16b9c34c9042dbfb7e0777f732c8c1
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ab5628c5a12d4672dac5c728f675b5632dba6df86a1d6646798efa398898966c
Found 1 unique certificates

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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.tomsmucenieks.asimplevibrator.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
425c3d2bcfb5ed4b3ad426ec7fe0506d.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<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.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | 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.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (com.tomsmucenieks.asimplevibrator.SplashActivity) 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.
3	Activity-Alias (com.tomsmucenieks.asimplevibrator.SplashActivityFake) 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.
4	Activity-Alias (com.tomsmucenieks.asimplevibrator.SplashActivityReal) 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.
5	Activity (com.tomsmucenieks.asimplevibrator.MainActivity) 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 (com.tomsmucenieks.asimplevibrator.MultiVibrateActivity) 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.
7	Activity (com.tomsmucenieks.asimplevibrator.OnlineActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/stfalcon/chatkit/messages/MessagesListAdapter.java com/tomsmucenieks/asimplevibrator/MultiVibrateActivity.java com/tomsmucenieks/asimplevibrator/utils/LinkUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/epicgames/mobile/eossdk/EOSSDK.java com/github/appintro/internal/LogHelper.java com/leff_shadowed/midi/MidiFile.java com/leff_shadowed/midi/MidiTrack.java com/leff_shadowed/midi/event/MidiEvent.java com/leff_shadowed/midi/event/meta/GenericMetaEvent.java com/leff_shadowed/midi/event/meta/MetaEvent.java com/leff_shadowed/midi/examples/EventPrinter.java com/leff_shadowed/midi/examples/MidiFileFromScratch.java com/leff_shadowed/midi/examples/MidiManipulation.java com/tomsmucenieks/asimplevibrator/EosWrapper.java com/tomsmucenieks/asimplevibrator/IntroActivity.java com/tomsmucenieks/asimplevibrator/MainActivity.java com/tomsmucenieks/asimplevibrator/background/NotificationService.java com/tomsmucenieks/asimplevibrator/utils/BillingWrapper.java com/tomsmucenieks/asimplevibrator/utils/MidiPlayer.java com/tomsmucenieks/asimplevibrator/utils/VibrationFileUtils.java me/everything/android/ui/overscroll/OverScrollBounceEffectDecoratorBase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	com/tomsmucenieks/asimplevibrator/utils/RandomUtils.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/tomsmucenieks/asimplevibrator/enums/Enums.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/epicgames/mobile/eossdk/EOSSDK.java com/tomsmucenieks/asimplevibrator/MainActivity.java com/tomsmucenieks/asimplevibrator/fragments/SettingsFragment.java com/tomsmucenieks/asimplevibrator/utils/LinkUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/tomsmucenieks/asimplevibrator/MainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/epicgames/mobile/eossdk/EOSSDK.java
00013	Read file and put it into a stream	file	com/leff_shadowed/midi/MidiFile.java com/tomsmucenieks/asimplevibrator/utils/VibrationFileUtils.java
00012	Read data and put it into a buffer stream	file	com/leff_shadowed/midi/MidiFile.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://best-vibrator-pro.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/61460459223/namespaces/firebase:fetch?key=AIzaSyDCjDGrI8GbkQeKijXRPyPaXAzSzbye33c is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'isLobbies': 'true'}, 'state': 'UPDATE', 'templateVersion': '4'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
apps.xtactic.net	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
onelink.to	ok	**IP:** 178.128.140.200 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
soundcloud.com	ok	**IP:** 18.238.96.6 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xtactic.net	ok	**IP:** 172.67.202.38 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
best-vibrator-pro.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
goo.gl	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
support@xtactic.net	com/tomsmucenieks/asimplevibrator/fragments/SettingsFragment.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://best-vibrator-pro.firebaseio.com"
"google_api_key" : "AIzaSyDCjDGrI8GbkQeKijXRPyPaXAzSzbye33c"
"google_crash_reporting_api_key" : "AIzaSyDCjDGrI8GbkQeKijXRPyPaXAzSzbye33c"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE
49f946663a8deb7054212b8adda248c6
V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=
3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=

POSSIBLE SECRETS
36864200e0eaf5284d884a0e77d31646
Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl
QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5
JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=
Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=
6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY
fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W
a0784d7a4716f3feb4f64e7f4b39bf04
e39393ce62804df98d2875b89aade3d5
67eea66c80a5439c844ed2a83ae2160f

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=
u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=
bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRlI5KKEyt63x08=
eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=
vvYcBqgl4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg
ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc
af60eb711bd85bc1e4d3e0a462e074eea428a8
oMWPsiFnko7JIQivd/SGXGobWnc06XcidiDsEhiwmoI
5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11
0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
KvkOAoII09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI

POSSIBLE SECRETS
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHclJcD0mydl5RKvI49M
tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57
FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
TvLSh+Eka5RyCXMK4IvAvP4vfksx/KqJwxjzSKu7qQs=
Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=
470fa2b4ae81cd56ecbcda9735803434cec591fa
AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=
GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XllzkH3EMVH
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

POSSIBLE SECRETS
gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B
6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=
WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK
K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=
9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7IORvVFb3+Q=
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ
NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=
0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=
M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=

POSSIBLE SECRETS
xyza78917UEnbDR8iGFsfycP3QpFz0NM
iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 4d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313074 16e64726f6964301e170d303830383231323331333333345a170d333630313037323331333333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 4d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313074 16e64726f69643082012030d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 4d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313074 16e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010 1006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f609ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
B3EEABB8EE11C2BE770B684D95219ECB
SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD
d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK

POSSIBLE SECRETS
g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1XI+70++CdiHkDZKRlUPQw
lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=
c103703e120ae8cc73c9248622f3cd1e
SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e060355040313 07416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b300906035504061302555331133011060355040813 0a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e060355040313 07416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
db65afb89a1f41fa85cddde47b3b0e06
SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=

PLAYSTORE INFORMATION

Title: Vibrator: Strong Vibration App

Score: 4.44335 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.tomsmucenieks.asimplevibrator

Developer Details: xTactic, xTactic, None, https://xtactic.net/apps/, support@xtactic.net,

Release Date: Oct 16, 2016 **Privacy Policy:** Privacy link

Description:

Introducing Vibe - intense vibrator app for massage and relax! Now with ONLINE CHAT & MASSAGE! TRY NOW! Have you ever wanted a personal massager? Well, now you can turn your phone into a professional massaging device with this easy-to-use strong vibrator app! No more worries about aching back. This app does it all! Tutorial: Just launch the vibrator app, tap the switch, put the phone on your desired area and relax! :) Features: - 10 unique vibration patterns. Including intense music rhythm patterns! - Almost unlimited vibration modes. You can set your own pace and relax! - Vibe Together - Meet, Chat and Vibe with other people together with this never-seen-before online vibrator feature! - Change intensity from peaceful to mega strong vibration - Vibrate in background while using other apps - Vibrate while screen is off - Create your own intense vibration patterns - Unlimited possibilities. - Share and import custom vibration patterns! - Mask app as a Simple Calculator for extra privacy Use this massage vibrator to: - Relax muscles - Meditate - Calm yourself - Increase happiness - Reduce anxiety and stress - Sleep - Relief back pain Everything in this strong vibration app is free to use. Enjoy! You can create, import and share vibration patterns as .vibr files. If you've found any bugs, please contact us on developer's e-mail!

SCAN LOGS

Timestamp	Event	Error
2025-09-01 10:32:05	Generating Hashes	OK
2025-09-01 10:32:05	Extracting APK	OK
2025-09-01 10:32:05	Unzipping	OK
2025-09-01 10:32:05	Parsing APK with androguard	OK

2025-09-01 10:32:06	Extracting APK features using aapt/aapt2	OK
2025-09-01 10:32:06	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 10:32:08	Parsing AndroidManifest.xml	OK
2025-09-01 10:32:08	Extracting Manifest Data	OK
2025-09-01 10:32:08	Manifest Analysis Started	OK
2025-09-01 10:32:08	Performing Static Analysis on: Vibrator Strong (com.tomsmucenieks.asimplevibrator)	OK
2025-09-01 10:32:08	Fetching Details from Play Store: com.tomsmucenieks.asimplevibrator	OK
2025-09-01 10:32:09	Checking for Malware Permissions	OK
2025-09-01 10:32:09	Fetching icon path	OK
2025-09-01 10:32:09	Library Binary Analysis Started	OK
2025-09-01 10:32:09	Reading Code Signing Certificate	OK

2025-09-01 10:32:10	Running APKiD 2.1.5	OK
2025-09-01 10:32:16	Detecting Trackers	OK
2025-09-01 10:32:21	Decompiling APK to Java with JADX	OK
2025-09-01 10:33:24	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 10:33:24	Decompiling classes2.dex with JADX	OK
2025-09-01 10:33:35	Decompiling classes4.dex with JADX	OK
2025-09-01 10:33:37	Decompiling classes.dex with JADX	OK
2025-09-01 10:33:47	Decompiling classes3.dex with JADX	OK
2025-09-01 10:33:58	Decompiling classes2.dex with JADX	OK
2025-09-01 10:34:10	Decompiling classes4.dex with JADX	OK

2025-09-01 10:34:12	Decompiling classes.dex with JADX	OK
2025-09-01 10:34:27	Decompiling classes3.dex with JADX	OK
2025-09-01 10:34:42	Converting DEX to Smali	OK
2025-09-01 10:34:42	Code Analysis Started on - java_source	OK
2025-09-01 10:34:52	Android SBOM Analysis Completed	OK
2025-09-01 10:34:56	Android SAST Completed	OK
2025-09-01 10:34:56	Android API Analysis Started	OK
2025-09-01 10:34:59	Android API Analysis Completed	OK
2025-09-01 10:35:00	Android Permission Mapping Started	OK
2025-09-01 10:35:03	Android Permission Mapping Completed	OK

2025-09-01 10:35:17	Android Behaviour Analysis Started	OK
2025-09-01 10:35:24	Android Behaviour Analysis Completed	OK
2025-09-01 10:35:24	Extracting Emails and URLs from Source Code	OK
2025-09-01 10:35:25	Email and URL Extraction Completed	OK
2025-09-01 10:35:25	Extracting String data from APK	OK
2025-09-01 10:35:25	Extracting String data from Code	OK
2025-09-01 10:35:25	Extracting String values and entropies from Code	OK
2025-09-01 10:35:31	Performing Malware check on extracted domains	OK
2025-09-01 10:35:33	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.