Signal 4.32.8

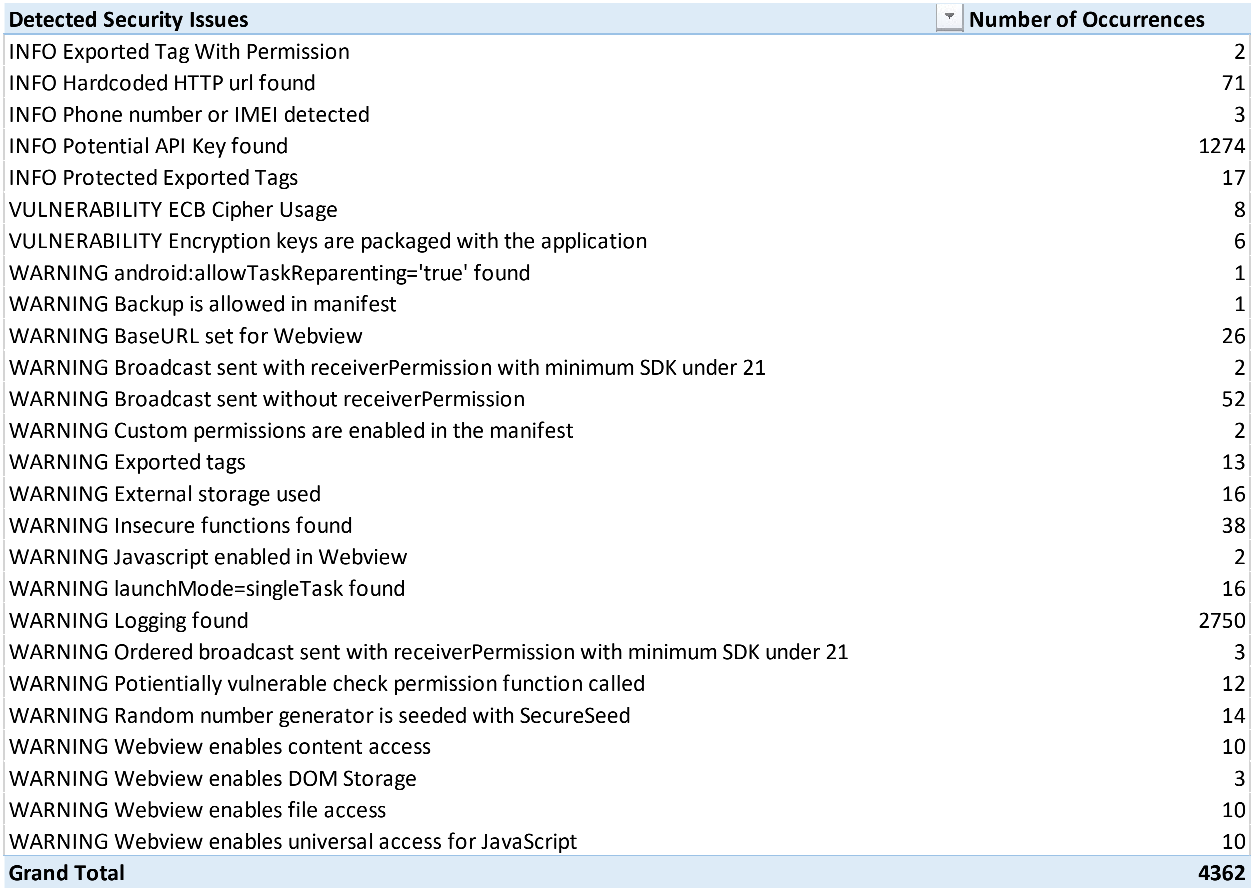
February 02nd, 2018.

Description: This is a review of the Signal Private Messenger 4.32.8. After performing a static analysis of the app, vulnerabilities were identified related to device identification, file permissions, code execution, hash algorithm, and log activities. Additional results shows the use of 29 permissions without an android reference definition.

These analyses are aligned with the Common Weakness Enumerations (CWE) such as:

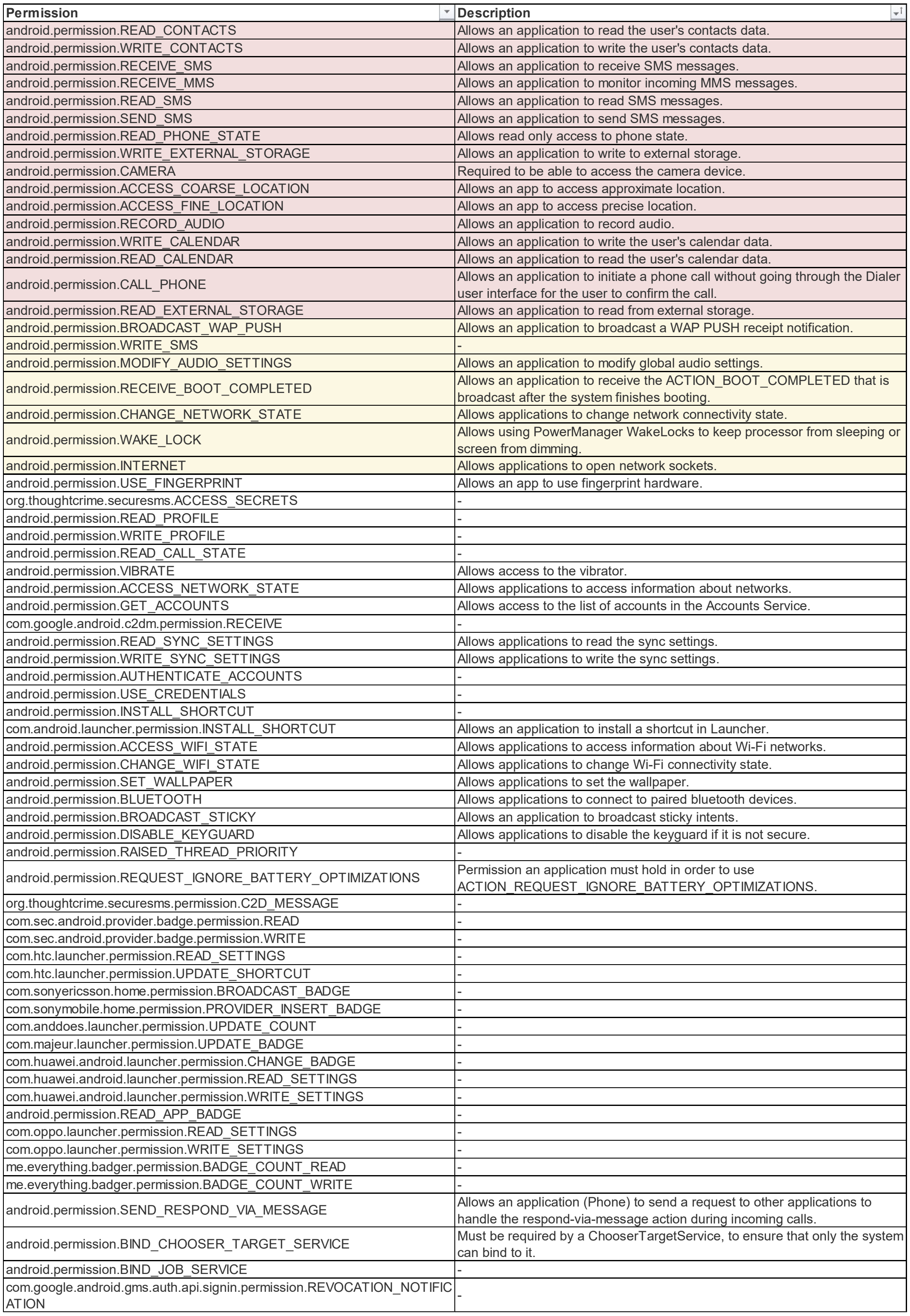
a) 312 (Cleartext Storage of Sensitive Information),
b) 327 (Use of a Broken or Risky Cryptographic Algorithm),
c) 532 (Information Exposure Through Log Files),
d) 330 (Use of Insufficiently Random Values),
e) 200 (Information Exposure),
f) 276 (Incorrect Default Permissions), and
g) 89 (Improper Neutralization of Special Elements used in an SQL Command - 'SQL Injection').

Summary of Vulnerabilities



Detected Security Issues	Number of Occurrences
INFO Exported Tag With Permission	2
INFO Hardcoded HTTP url found	71
INFO Phone number or IMEI detected	3
INFO Potential API Key found	1274
INFO Protected Exported Tags	17
VULNERABILITY ECB Cipher Usage	8
VULNERABILITY Encryption keys are packaged with the application	6
WARNING android:allowTaskReparenting='true' found	1
WARNING Backup is allowed in manifest	1
WARNING BaseURL set for Webview	26
WARNING Broadcast sent with receiverPermission with minimum SDK under 21	2
WARNING Broadcast sent without receiverPermission	52
WARNING Custom permissions are enabled in the manifest	2
WARNING Exported tags	13
WARNING External storage used	16
WARNING Insecure functions found	38
WARNING Javascript enabled in Webview	2
WARNING launchMode=singleTask found	16
WARNING Logging found	2750
WARNING Ordered broadcast sent with receiverPermission with minimum SDK under 21	3
WARNING Potientially vulnerable check permission function called	12
WARNING Random number generator is seeded with SecureSeed	14
WARNING Webview enables content access	10
WARNING Webview enables DOM Storage	3
WARNING Webview enables file access	10
WARNING Webview enables universal access for JavaScript	10
Grand Total	**4362**

Summary of Permissions



Permission	Description
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data.
android.permission.WRITE_CONTACTS	Allows an application to write the user's contacts data.
android.permission.RECEIVE_SMS	Allows an application to receive SMS messages.
android.permission.RECEIVE_MMS	Allows an application to monitor incoming MMS messages.
android.permission.READ_SMS	Allows an application to read SMS messages.
android.permission.SEND_SMS	Allows an application to send SMS messages.
android.permission.READ_PHONE_STATE	Allows read only access to phone state.
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.
android.permission.CAMERA	Required to be able to access the camera device.
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location.
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location.
android.permission.RECORD_AUDIO	Allows an application to record audio.
android.permission.WRITE_CALENDAR	Allows an application to write the user's calendar data.
android.permission.READ_CALENDAR	Allows an application to read the user's calendar data.
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
android.permission.BROADCAST_WAP_PUSH	Allows an application to broadcast a WAP PUSH receipt notification.
android.permission.WRITE_SMS	-
android.permission.MODIFY_AUDIO_SETTINGS	Allows an application to modify global audio settings.
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state.
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.
android.permission.INTERNET	Allows applications to open network sockets.
android.permission.USE_FINGERPRINT	Allows an app to use fingerprint hardware.
org.thoughtcrime.securesms.ACCESS_SECRETS	-
android.permission.READ_PROFILE	-
android.permission.WRITE_PROFILE	-
android.permission.READ_CALL_STATE	-
android.permission.VIBRATE	Allows access to the vibrator.
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks.
android.permission.GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.
com.google.android.c2dm.permission.RECEIVE	-
android.permission.READ_SYNC_SETTINGS	Allows applications to read the sync settings.
android.permission.WRITE_SYNC_SETTINGS	Allows applications to write the sync settings.
android.permission.AUTHENTICATE_ACCOUNTS	-
android.permission.USE_CREDENTIALS	-
android.permission.INSTALL_SHORTCUT	-
com.android.launcher.permission.INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher.
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state.
android.permission.SET_WALLPAPER	Allows applications to set the wallpaper.
android.permission.BLUETOOTH	Allows applications to connect to paired bluetooth devices.
android.permission.BROADCAST_STICKY	Allows an application to broadcast sticky intents.
android.permission.DISABLE_KEYGUARD	Allows applications to disable the keyguard if it is not secure.
android.permission.RAISED_THREAD_PRIORITY	-
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	Permission an application must hold in order to use ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
org.thoughtcrime.securesms.permission.C2D_MESSAGE	-
com.sec.android.provider.badge.permission.READ	-
com.sec.android.provider.badge.permission.WRITE	-
com.htc.launcher.permission.READ_SETTINGS	-
com.htc.launcher.permission.UPDATE_SHORTCUT	-
com.sonyericsson.home.permission.BROADCAST_BADGE	-
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	-
com.anddoes.launcher.permission.UPDATE_COUNT	-
com.majeur.launcher.permission.UPDATE_BADGE	-
com.huawei.android.launcher.permission.CHANGE_BADGE	-
com.huawei.android.launcher.permission.READ_SETTINGS	-
com.huawei.android.launcher.permission.WRITE_SETTINGS	-
android.permission.READ_APP_BADGE	-
com.oppo.launcher.permission.READ_SETTINGS	-
com.oppo.launcher.permission.WRITE_SETTINGS	-
me.everything.badger.permission.BADGE_COUNT_READ	-
me.everything.badger.permission.BADGE_COUNT_WRITE	-
android.permission.SEND_RESPOND_VIA_MESSAGE	Allows an application (Phone) to send a request to other applications to handle the respond-via-message action during incoming calls.
android.permission.BIND_CHOOSER_TARGET_SERVICE	Must be required by a ChooserTargetService, to ensure that only the system can bind to it.
android.permission.BIND_JOB_SERVICE	-
com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION	-

References:

1. Androwarn Report

https://github.com/GitHubAssessments/CVE_Assessment_02_2019/blob/master/Signal_Androwarn_Report.pdf

2. MOBSF Report

https://github.com/GitHubAssessments/CVE_Assessment_02_2019/blob/master/Signal_MOBSF_Report.pdf

3. QARK Report

https://github.com/GitHubAssessments/CVE_Assessment_02_2019/blob/master/Signal_QARK_Report.pdf