ANDROID STATIC ANALYSIS REPORT

PunchAlert (5.5.3.0)

File Name:	PunchAlert_v5.5.3.0_apkpure.com.xapk
Package Name:	in.punch.alert
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	10/421
Scan Date:	Feb. 20, 2022, 6:13 p.m.

FILE INFORMATION

File Name: PunchAlert_v5.5.3.0_apkpure.com.xapk
Size: 8.26MB
MD5: 6aea7af02091d781ff8e255f0a7f6424

SHA1: ecbad4fc48772b90aef23a2d38f10a7b6b46ffc4
SHA256: ce633196c2e18ef5943f383cce08d3385d86d41b9d9b1b2beb4d0480d8cd5bec

APP INFORMATION

App Name: PunchAlert
Package Name: in.punch.alert
Main Activity: in.punch.alert.ui.launch.SplashScreenActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 5.5.3.0
Android Version Code: 56000

APP COMPONENTS

Activities: 103
Services: 23
Receivers: 11
Providers: 10
Exported Activities: 1
Exported Services: 5
Exported Receivers: 6
Exported Providers: 1

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=NC, L=Charlotte, O=Punch Technologies, Inc., OU=Unknown, CN=Unknown

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-12-19 18:46:13+00:00
Valid To: 2041-05-06 18:46:13+00:00
Issuer: C=US, ST=NC, L=Charlotte, O=Punch Technologies, Inc., OU=Unknown, CN=Unknown
Serial Number: 0x52b33ef5
Hash Algorithm: sha1
md5: 921a99a02bee87a766297d3f150bfc82
sha1: 384e29f9a8a2f79c08950bf8ec0ca28df4d061f5
sha256: e95220bc09920ea05cf08567948975a04c0aa6365f80ded7dadf5eae92b7fe0e
sha512: 6a219518fef6e40d23554885807d334548c406526bb093670ae00207013ff8f1415b54650c16c6148affc3c217d319a331798b35744c32ef931f70aeef937490
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b077be13d94fbe19b19a572bf068f225d81813806e833d33bb23d2a788abdc17

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.USE_SIP	dangerous	make/receive Internet calls	Allows an application to use the SIP service to make/receive Internet calls.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal		Marker permission for applications that wish to access notification policy.
in.punch.alert.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check
	Compiler	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.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name 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>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
in.punch.alert.ui.launch.SplashScreenActivity	Schemes: @string/custom_uri_scheme://,

ACTIVITY	INTENT
com.okta.oidc.OktaRedirectActivity	Schemes: com.okta.dev-889080://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Service (org.abtollc.service.ABTOSipService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
2	Service (in.punch.alert.service.pushnotifications.FirebaseInstanceIDService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
3	Service (in.punch.alert.service.pushnotifications.FirebaseMessageReciever) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (com.onesignal.BootUpReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (com.onesignal.UpgradeReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
7	Broadcast Receiver (com.pushwoosh.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Service (com.pushwoosh.FcmRegistrationService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
9	Service (com.pushwoosh.PushFcmIntentService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
10	Content Provider (com.pushwoosh.PushwooshSharedDataProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (com.okta.oidc.OktaRedirectActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	High Intent Priority (999) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cp.pushwoosh.com	good	**IP:** 88.198.209.124 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
s.api.pushwoosh.com	good	**IP:** 78.47.243.139 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map
onesignal.com	good	**IP:** 104.18.225.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
punchalert.com	good	**IP:** 52.165.174.123 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
punchalert-83d0d.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
docs.google.com	good	**IP:** 142.251.33.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdk.hockeyapp.net	good	**IP:** 40.70.164.17 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
api.onesignal.com	good	**IP:** 104.18.225.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	good	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gl	good	**IP:** 142.251.33.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	good	**IP:** 172.217.14.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.punchalert.com	good	**IP:** 52.242.124.17 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
go.pushwoosh.com	good	**IP:** 88.198.209.124 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
maps.googleapis.com	good	**IP:** 142.251.33.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
punchalert.okta.com	good	**IP:** 34.223.95.130 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.youtube.com	good	**IP:** 172.217.14.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
file:///android_asset/	com/bumptech/glide/load/b/a.java
data:image	com/bumptech/glide/load/b/e.java
https://www.example.com	com/okta/oidc/OktaAuthenticationActivity.java
https://onesignal.com/android_frame.html	com/onesignal/be.java
https://api.onesignal.com/	com/onesignal/bk.java
data:JSON	com/onesignal/br.java
https://cp.pushwoosh.com/json/1.3/ https://%s.api.pushwoosh.com/json/1.3/	com/pushwoosh/a/ab.java
javascript:%s javascript:_pwCallbackHelper.invokeCallback(	com/pushwoosh/inapp/view/a/a.java

javascript:%s();
javascript:%s('%s');
	com/pushwoosh/inapp/view/a/e.java

javascript:window.pushwoosh	com/pushwoosh/inapp/view/a/g.java
https://sdk.hockeyapp.net/	com/pushwoosh/internal/crash/j.java
https://goo.gl/UVJKfp	com/pushwoosh/internal/d/c.java

URL	FILE
https://goo.gl/KZa9M4	com/pushwoosh/internal/d/d.java
https://go.pushwoosh.com/content/%s	com/pushwoosh/notification/d/b/c.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/api/v3/models/response/OrganisationDetailsModel.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/c.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/EmergencyMapActivity.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/g.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/h.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/UserProfileActivity.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/responder/e.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/responder/f.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/responder/i.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activeemergency/responder/ManageEmergencyActivity.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/activity/f.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/b/b.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/b/c.java

URL	FILE
http://play.google.com/store/apps/details?id= https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/home/HomeActivity.java
https://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true&language=	in/punch/alert/ui/location/a.java
https://punchalert.okta.com	in/punch/alert/ui/login/PlainActivity.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/navigation/c.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/post/announcements/CreateAnnouncementActivity.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id= https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/post/announcements/PostAnnouncementActivity.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/post/tips/TipCategoryActivity.java
https://app.punchalert.com/_handlers/ShowCompanyLogo.ashx?id=	in/punch/alert/ui/reportemergency/d.java
https://app.punchalert.com/_handlers/ShowUserImage.ashx?id=	in/punch/alert/ui/settings/SettingsActivity.java
https://play.google.com/store/apps/details?id=	in/punch/alert/ui/subscriptions/ManageSubscriptionsActivity.java
https://punchalert.com/911plus	in/punch/alert/ui/subscriptions/SubscriptionsActivity.java
https://www.youtube.com/watch?v=LWPzb-xZRPo	in/punch/alert/ui/upgradeto911/j.java
https://app.punchalert.com/	in/punch/alert/ui/viewplan/DownloadPlanService.java

URL	FILE
https://docs.google.com/gview?embedded=true&url= javascript:(function()	in/punch/alert/ui/viewplan/PDFWebViewActivity.java
https://punchalert-83d0d.firebaseio.com https://app.punchalert.com/_policies/EULA.html https://app.punchalert.com/_policies/privacy.htm https://punchalert.com/tou/	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://punchalert-83d0d.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@punchalert.com fakeemail@gmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
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
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193
Pushwoosh		https://reports.exodus-privacy.eu.org/trackers/39

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above."
"feed_ipaws_data_obtained" : "feed_ipaws_data_obtained"

POSSIBLE SECRETS
"firebase_database_url" : "https://punchalert-83d0d.firebaseio.com"
"google_api_key" : "AIzaSyA21hrqxNcHSLZ4nwgqwrXIsAIKzaiCyJE"
"google_crash_reporting_api_key" : "AIzaSyA21hrqxNcHSLZ4nwgqwrXIsAIKzaiCyJE"
"ipaws_no_amber" : "No amber alerts."
"ipaws_no_other" : "No other updates."
"ipaws_no_weather" : "No weather updates."
"load_ipaws" : "load_ipaws"
"login_credentials_invalid" : "That’s not the correct password. Sorry!"
"okta_reset_password" : "Okta Reset Password"
"password" : "Password"
"places_maps_key" : "AIzaSyA5EP3WossJT-mbZ3OErCbFI1I5TQwpU_Q"
"punch_beacon_app_token" : "b0dcf6fcd5c4da6ba9035a2095b928c9"
"pwd_criteria_txt" : "Minimum 8 characters, 1 number, 1 upper and lowercase letter"
"pwd_match_err_txt" : "These password doesn't match"
"reset_password" : "Send link to reset password to: %s"

POSSIBLE SECRETS
"settings_password" : "Password"
"showIPaws" : "showIpaws"
"showIPawsAmber" : "showIPawsAmber"
"showIPawsOther" : "showIPawsOther"
"showIPawsWeather" : "showIPawsWeather"
"template_resend_password" : "Send link to reset password to: Fakeemail@gmail.com"

PLAYSTORE INFORMATION

Title: PunchAlert

Score: 2.7142856 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Tools **Play Store URL:** in.punch.alert

Developer Details: Punch Technologies, Inc., Punch+Technologies,+Inc., 806 Tyvola Rd. Charlotte, NC 28217, http://www.punchalert.com, contact@punchalert.com,

Release Date: Apr 2, 2014 **Privacy Policy:** Privacy link

Description:

PunchAlert is the safety app for you, your neighbors and your entire community. It's the easiest way to stay safe, informed, and connected to the organizations in your area. Now with 911+, you can connect to local official responders better than ever before. People everywhere are using PunchAlert to: - Connect to the police while simultaneously alerting friends and family. - Quickly report a break-in, suspicious activity, vandalism, a scam or theft - Connect with places or organizations in their city that already use PunchAlert for emergency preparation and management - Post tips or events like local blood drives and neighborhood watch meetings - Help bring together lost pets with their owners - Live stress free knowing they have a smart panic button always one tap away Organizations all over the country are using PunchAlert to: - Manage emergencies from your mobile device leveraging responder chat, mass notifications, emergency plan distribution, real-time location capture inside geo-fences, crowdsourced photos and videos, and more. PunchAlert allows organizations to communicate more efficiently and resolve incidents faster, all the while creating a detailed record and report of the incident. - Crowdsource safety tips and incidents from employees, customers, or visitors. - Send announcements to employees, customers, students, or guests. - Create a community of safety Notes: Some features of PunchAlert require a data connection either through WiFi or a cellular network. During an emergency incident, continued use of GPS running in the background can decrease battery life. We monitor battery life to account for such scenarios. In the case of issues with 911+ call quality, we provide a link to call 911 outside of PunchAlert using cellular. Emoji icons supplied by EmojiOne.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.4.5 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.