MOBSF

ANDROID STATIC ANALYSIS REPORT

iConnect (0.0.13)

File Name:	iConnect_0.0.13_apkcombo.com.xapk
Package Name:	com.growatiopex.iconnect
Scan Date:	April 6, 2025, 8:56 p.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	12	2	3	1

FILE INFORMATION

File Name: iConnect_0.0.13_apkcombo.com.xapk
Size: 15.32MB
MD5: a23244ea3909eaa941d4abff20ab85a4
SHA1: e6462a922122f6aa239d222e5d3030ecdfef539c
SHA256: 9a6d932574a661c6d59eb38ca3a109babffc17b6a6b13ff147a99b68d2bd3031

APP INFORMATION

App Name: iConnect
Package Name: com.growatiopex.iconnect
Main Activity: com.growatiopex.iconnect.MainActivity
Target SDK: 33
Min SDK: 24
Max SDK:
Android Version Name: 0.0.13

Android Version Code: 13

APP COMPONENTS

Activities: 7
Services: 9
Receivers: 4
Providers: 3
Exported Activities: 4
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
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: 2022-11-30 15:12:19+00:00
Valid To: 2052-11-30 15:12:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x52e47bb2347b3128503a76972ea0e8fa8724d789
Hash Algorithm: sha256
md5: 7b55decd872ce660b4a877066d8a4186
sha1: 536b6520eee333fdb03954613f081d496cb2ffb5
sha256: 8ed45d56798392fbd5d4a745c120a6b128ed96510e52be9240aae3372efca7ec
sha512: 2c2076ac101eddb0ce7f9ba6f24e789014b5707a9b12047672b4c19cee8f5be5f5f81781aa283c8d93d163625910d0b43dd35b66bb637804b4c35463c0a219a0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 80a25fb824e56a153ee69e139936a5a1cdb7e8e58ad882f76c339ba19edb566d
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.growatiopex.iconnect.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-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.TAGS check
SIM operator check
network operator name 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>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>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
possible Build.SERIAL 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
com.growatiopex.iconnect.MainActivity	Schemes: http://, https://, Hosts: digital.growatiopex.com, Path Prefixes: /,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.growatiopex.iconnect://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

ACTIVITY	INTENT
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: 1 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 3 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
4	App Link assetlinks.json file not found [android:name=com.growatiopex.iconnect.MainActivity] [android:host=http://digital.growatiopex.com]	high	App Link asset verification URL (http://digital.growatiopex.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 403). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
5	App Link assetlinks.json file not found [android:name=com.growatiopex.iconnect.MainActivity] [android:host=https://digital.growatiopex.com]	high	App Link asset verification URL (https://digital.growatiopex.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 403). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
6	Activity (org.apache.cordova.firebase.OnNotificationReceiverActivity) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.
8	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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
9	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]	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	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
11	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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: **3** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				by/chemerisuk/cordova/firebase/FirebaseDynamicLinksPlugin.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultIma

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	geHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/ionicframework/cordova/webview/AndroidProtocolHandler.java com/ionicframework/cordova/webview/IonicWebViewE

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ngine.java com/monicframework/cordova/webview/WebViewLocalServer.java cordova/plugin/RequestLocationAccuracy.java cordova/plugins/Diagnostic.java cordova/plugins/Diagnostic_Bluetooth.java cordova/plugins/Diagnostic_Camera.java cordova/plugins/Diagnostic_External_Storage.java cordova/plugins/Diagnostic_Location.java cordova/plugins/Diagnostic_NFC.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/Diagnostic_Wifi.java defpackage/Crypto.java defpackage/NativeStorage.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java
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	cordova/plugins/Diagnostic.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/TransportFrameUtil.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cordova/plugins/Diagnostic.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/ionicframework/cordova/webview/AndroidProtocolHandler.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java okio/Okio.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	by/chemerisuk/cordova/firebase/FirebaseDynamicLinksPlugin.java cordova/plugins/Diagnostic_Notifications.java
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/okhttp/internal/Platform.java
00163	Create new Socket and connecting to it	socket	io/grpc/okhttp/internal/Platform.java
00004	Get filename and put it to JSON object	file collection	cordova/plugins/Diagnostic.java
00096	Connect to a URL and set request method	command network	com/ionicframework/cordova/webview/WebViewLocalServer.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/ionicframework/cordova/webview/WebViewLocalServer.java
00094	Connect to a URL and read data from it	command network	com/ionicframework/cordova/webview/WebViewLocalServer.java
00108	Read the input stream from given URL	network command	com/ionicframework/cordova/webview/WebViewLocalServer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	cordova/plugins/Diagnostic_Notifications.java
00036	Get resource file from res/raw directory	reflection	com/ionicframework/cordova/webview/AndroidProtocolHandler.java cordova/plugins/Diagnostic_Notifications.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://iconnectapp-57353-default-rtdb.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/93192277194/namespaces/firebase:fetch?key=AIzaSyD6Txx-Z8PTxnalfeBlgBigv5bUUsI83QY. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	4/44	android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, 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

DOMAIN	STATUS	GEOLOCATION
iconnectapp-57353-default-rtdb.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://iconnectapp-57353-default-rtdb.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyD6Txx-Z8PTxnalfeBlgBigv5bUUsI83QY"
"google_crash_reporting_api_key" : "AIzaSyD6Txx-Z8PTxnalfeBlgBigv5bUUsI83QY"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
470fa2b4ae81cd56ecbcda9735803434cec591fa
1157920892103562487626974469494075735300861434152903141955336313088670978539 51

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

PLAYSTORE INFORMATION

Title: iConnect

Score: None **Installs:** 1,000+ **Price:** 0 **Android Version Support:** **Category:** Business **Play Store URL:** com.growatiopex.iconnect

Developer Details: iOPEX Technologies Pvt Ltd, iOPEX+Technologies+Pvt+Ltd, None, https://iopex.com/, mobile.dev@iopex.com,

Release Date: Dec 15, 2022 **Privacy Policy:** Privacy link

Description:

The iOPEX iConnect app is designed for employees to connect with the company and their coworkers in a more engaging way. With this app, employees can check the latest updates of the company, see engagement activities, photos, and videos, and wish their peers birthdays and work anniversaries. This app helps create a more positive and connected work environment for employees with ease. iOPEX iConnect enables users to stay updated with the latest news and happenings of iOPEX. It provides quick access to the company's latest happenings, engagement, blog and more. Additionally, it offers to push notifications for important news and updates.

SCAN LOGS

Timestamp	Event	Error
2025-04-06 20:56:22	Generating Hashes	OK
2025-04-06 20:56:22	Extracting APK	OK
2025-04-06 20:56:22	Unzipping	OK
2025-04-06 20:56:23	Parsing APK with androguard	OK
2025-04-06 20:56:23	Extracting APK features using aapt/aapt2	OK
2025-04-06 20:56:23	Getting Hardcoded Certificates/Keystores	OK
2025-04-06 20:56:26	Parsing AndroidManifest.xml	OK
2025-04-06 20:56:26	Extracting Manifest Data	OK
2025-04-06 20:56:26	Manifest Analysis Started	OK

2025-04-06 20:56:26	Reading Network Security config from network_security_config.xml	OK
2025-04-06 20:56:26	Parsing Network Security config	OK
2025-04-06 20:56:26	Performing Static Analysis on: iConnect (com.growatiopex.iconnect)	OK
2025-04-06 20:56:26	Fetching Details from Play Store: com.growatiopex.iconnect	OK
2025-04-06 20:56:26	Checking for Malware Permissions	OK
2025-04-06 20:56:26	Fetching icon path	OK
2025-04-06 20:56:26	Library Binary Analysis Started	OK
2025-04-06 20:56:26	Reading Code Signing Certificate	OK
2025-04-06 20:56:27	Running APKiD 2.1.5	OK
2025-04-06 20:56:32	Detecting Trackers	OK
2025-04-06 20:56:37	Decompiling APK to Java with JADX	OK

2025-04-06 20:57:27	Converting DEX to Smali	OK
2025-04-06 20:57:27	Code Analysis Started on - java_source	OK
2025-04-06 20:57:29	Android SBOM Analysis Completed	OK
2025-04-06 20:58:06	Android SAST Completed	OK
2025-04-06 20:58:06	Android API Analysis Started	OK
2025-04-06 20:58:09	Android API Analysis Completed	OK
2025-04-06 20:58:09	Android Permission Mapping Started	OK
2025-04-06 20:58:13	Android Permission Mapping Completed	OK
2025-04-06 20:58:14	Android Behaviour Analysis Started	OK
2025-04-06 20:58:16	Android Behaviour Analysis Completed	OK
2025-04-06 20:58:16	Extracting Emails and URLs from Source Code	OK

2025-04-06 20:58:17	Email and URL Extraction Completed	OK
2025-04-06 20:58:17	Extracting String data from APK	OK
2025-04-06 20:58:17	Extracting String data from Code	OK
2025-04-06 20:58:17	Extracting String values and entropies from Code	OK
2025-04-06 20:58:21	Performing Malware check on extracted domains	OK
2025-04-06 20:58:22	Saving to Database	OK
2025-04-06 20:59:12	Unzipping	OK

Report Generated by - MobSF v4.3.2

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.