報道関係者各位
プレスリリース

2016 年 7 月 29 日
リスクファインダー株式会社

第三者モジュール情報を強化
Android アプリの脆弱性診断 Web サービス
「RiskFinder 6.0（2016 年 7 月版）が 7 月 29 日提供開始

リスクファインダー株式会社(東京都台東区、代表取締役：谷口 岳、／sMedio（東証マザーズ：3913））（以下 リスクファインダー)は、2016 年 7 月 29 日（金）、Android アプリの脆弱性診断ウェブサービス「RiskFinder（リスクファインダー）」の最新版となる「RiskFinder6.0（2016 年 7 月版）」をリリースしました。

「RiskFinder6.0（2016 年 7 月版）」： http://www.riskfinder.co.jp/

【「RiskFinder」について】
「RiskFinder」は、Android アプリの脆弱性を診断する Web サービスです。ブラウザを経由してアプリケーションファイル(.apk ファイル)を「RiskFinder」サーバへアップロードするだけで、すぐに診断結果を得ることができます。「RiskFinder」は 2013 年 4 月のサービス開始以来、キャリアやアプリ開発会社、アプリ検証サービス会社など、多方面で利用されています。

【「RiskFinder6.0（2016 年 7 月版）」の変更点について】
今回の更新では、第三者モジュールの問題に対するリスク検出機能を強化しています。
最近のアプリ開発は、第三者が公開しているライブラリを利用して新たに開発するコード量を減らし、開発期間を短縮するのが主流になっています。しかしライブラリに脆弱性があった場合、これを利用するアプリも脆弱性を内包することになってしまいます。開発者はライブラリの内部実装を知る術がないため、アプリのリリース前にライブラリの脆弱性に気づくことはほぼ不可能であり、このような状況が脆弱性のあるアプリがリリースされてしまう一因となっています。
実際、アプリ開発用のフレームワークが提供するライブラリに脆弱性が発見された例が報告されています（*1,*2）。フレームワークが提供するライブラリに脆弱性がある場合、そのフレームワークを利用して開発されたすべてのアプリに脆弱性が埋め込まれることになり、これは非常に危険な状況といえます。
「RiskFinder」はアプリ内のライブラリの問題も検出しますので、このような状況への強力な対策となります。今回の更新では、ハイブリッドアプリ開発時に利用されるライブラリの脆弱性、および URLConnection や OkHttp といった通信に関連するクラス、ライブラリの脆弱性などを中心に、多くのアプリに影響があると思われるリスクを新たに検出対象として追加しています。
また第三者ライブラリ情報辞書にも、新たに 200 件以上の情報を追加しています。

リスクファインダーは、利用者へ安心して利用できるアプリを届けるため、常に「RiskFinder」を改善、強化し、アプリ開発作業を支援し続けています。

＊1 JVNDB-2015-006002　Apache Cordova Android におけるブリッジハイジャック攻撃を実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-006002.html
＊2 JVNDB-2015-000187　Apache Cordova におけるアクセス制限不備の脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-000187.html

【リスクファインダーについて】
社名　：　リスクファインダー株式会社
代表　：　代表取締役　谷口 岳
所在地：　東京都台東区東上野 2-1-1 フリーアネックスビル 8 階
URL　：　http://www.riskfinder.co.jp

【本件に関するお問い合わせ】
リスクファインダー株式会社　営業部
担当　：　島野 英司
電話　：　080-8873-8243
E-Mail：　info@riskfinder.co.jp