Kunai for Android 脆弱性診断結果

1 概要

2017 年 1 月 16 日 から 2017 年 1 月 27 日 に、ゲヒルン株式会社様にて Kunai for Android の脆弱性診断を実施いただきました。本資料にて診断結果を公開いたします。

2 検査結果サマリ

今回の診断では 1 件の脆弱性が検出されました。検出された脆弱性は、全て対抗策を提供いたしております。

3 検査対象について

2017 年 6 月にリリースいたしました Kunai for Android について、診断を実施いただきました。検査対象の機能は以下の通りです。

- シンク処理
- スケジュール機能
- 通知機能

4 診断観点について

以下の観点で診断いただきました。

診断項目	説明
データの安全な保存	認証情報やトークンなど利用者の秘密情報を保存する場合、第三者アプリが読み取れない場所に情報を暗号化して保存 しているかを検査します。
暗号化通信	認証情報やトークンなど利用者の秘密情報をリモートサー ビスと送受信する場合、暗号化通信を使用しているか、及び 通信先の検証が行われているか検査します。

入出力値検証	アプリケーションが SQL や XML 等を使用する場合に、SQL インジェクションや XML インジェクション等の可能性を検査 します。また端末内のファイルパス指定可能性等が確認された場合 は、ディレクトリトラバーサル等の可能性を検査します。
ロジック	特定機能の利用やポイント処理等がローカル側での判断に依存する可能性を検査します。
認証	端末 ID や SIM カード ID などの偽装可能な識別情報のみで利用者認証を行なっていないか検査します。
アプリ間連携	別のアプリと連携するための仕組みを使用している場合、情 報漏えい、サービス妨害、又は権限逸脱行為などの不正行為 を別のアプリから行なうことができるか検査します。
重要情報の意図しない出力	認証情報やトークンなどの利用者の秘密情報、又はプライバ シーに関わる情報が、プラットフォームや第三者ライブラリ の仕組みやデバッグ機能の残余によって、意図せず保存、リモートサービスに送信されている可能性を検査します。
暗号	暗号化を行う場合、採用する暗号キー、アルゴリズム、又は ロジックに問題がないか検査します。
機密情報のハードコード	暗号キー、API キー、又はパスワードなどがハードコードされていないか検査します。

5 検出された脆弱性について

5.1 検出された脆弱性への対応

検出された脆弱性は、公開前に改修いたしております。

5.2 検出された脆弱性について

1 件の脆弱性が検出されました。

脆弱性識別番号	CyVDB-1383
脆弱性タイプ	CWE-79：XSS
脆弱性の基本評価	•攻撃元区分(AV)：ネットワーク •攻撃条件の複雑さ(AC)：低 •必要な特権レベル(PR)：不要 •ユーザー関与レベル(UI)：要 •影響の想定範囲(Scope)：変更あり •機密性への影響(C)：低 •完全性への影響(I)：低 •可用性への影響(A)：なし
CVSS v3 基本値	6.1