kintone 脆弱性監査結果

1 概要

2020 年 12 月 14 日 から 2020 年 12 月 23 日に、ゲヒルン株式会社様にて kintone の脆弱性監査を実施いただきました。本資料にて監査結果を公開いたします。

2 監査結果サマリ

今回の監査では、新たな脆弱性は検出されませんでした。

3 監査対象について

2020 年 11 月にリリースいたしました kintone に関して、監査いただきました。監査対象の機能は以下の通りです。

- アクセス権の設定 API（アプリ/フィールド/レコード)
- プロセス管理の設定 API
- 一覧の設定 API
- アプリの一般設定 API
- アプリ復旧
- スペース復旧
- Excel/CSV ファイルからのアプリ作成
- 個人設定
- まとめて削除機能
- 日付(来年／来月／来週／明日／昨年／昨日)での絞り込み
- アプリ設定（計算式）
- アプリテンプレート
- アプリ管理者メモ

4 検証観点について

以下の観点で監査いただきました。

検証観点	詳細

認証セッション管理	認証セッションの発行、更新破棄といった一連サイクルにおける問題の有無を特定する他、強度の妥当性について監査します。
認証 Cookie	認証セッションに Cookie を利用している場合、Cookie に付与 される属性を監査します。
入出力値検証	SQL インジェクションやクロスサイトスクリプティング、ディレクトリトラバーサルなどの攻撃の起点になり得る入出力箇所を監査します。
リクエストの妥当性確認	ログインした利用者又は何らかの処理を実行しうる利用者が、悪意のあるサイトを経由したリクエストを送信することで、処理を意図せず実行させられてしまう可能性について監査します。
ロジック	課金やポイント処理等の不正利用可能性について監査します。
アクセス制御	各利用者に与えられた権限以外の操作ができる可能性ついて監査します。
重要な情報の管理	パスワードやクレジットカード、住所等の個人情報取り扱い方法の妥当性について監査します。
メール送信機能	メール送信機能が存在するサービスの場合、宛先や本文等を不正に設定されることでスパムメールに利用される可能性や、連続大量送信などの迷惑行為を受ける可能性について監査します。