kintone 脆弱性検査結果

1 概要

2014 年 2 月 5 日 から 2014 年 2 月 6 日に、サイバーディフェンス研究所様にて kintone の脆弱性検査を実施いただきました。本資料にて検査結果を公開いたします。

2 検査結果サマリ

今回の検査では 3 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

2014 年 4 月にリリースいたしました kintone に関して、公開前に検査いただきました。検査対象の機能は以下の通りです。

- kintone 4 月公開新規機能（https://kintone.cybozu.com/jp/support/update/140413.html）

4 検証観点について

以下の観点で検査いただきました。

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検査します
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 される属性を検査します。
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検査します。

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検査します。
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検査します。
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検査します。
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検査します。
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

第三者監査にて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

3 点の脆弱性が検出されました。

脆弱性タイプ	CWE-16 環境設定
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 •攻撃前の認証要否(Au)：単一 •機密性への影響(C)：部分的 •完全性への影響(I)：なし •可用性への影響(A)：なし
CVSS v2 基本値	4.0（レベルⅡ）

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)：中 •攻撃前の認証要否(Au)：単一 •機密性への影響(C)：なし •完全性への影響(I)：部分的 •可用性への影響(A)：なし
CVSS v2 基本値	3.5（レベルⅠ）

脆弱性タイプ	CWE-16 環境設定
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 •攻撃前の認証要否(Au)：単一 •機密性への影響(C)：部分的 •完全性への影響(I)：なし •可用性への影響(A)：なし
CVSS v2 基本値	4.0（レベルⅡ）