

kintone 脆弱性検査結果

1 概要

2013年8月20日から2013年8月22日にかけて、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。本ページにて検査結果について公開いたします。

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

2013年11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 ゲストスペース機能（11月追加実装部分）

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	各利用者には与えられた権限以外の操作ができる可能性について検査します。
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、公開前に改修するか、アドバイザリをリリースいたしております。

5.2 検出された脆弱性について

以下の2点の脆弱性が検出されました。

脆弱性タイプ	CWE-601 オープンリダイレクト
脆弱性の基本評価	<ul style="list-style-type: none"> ●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)：不要 ●機密性への影響(C)：部分的 ●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	6.4 (レベル II)

脆弱性タイプ	CWE-20 不適切な入力確認
脆弱性の基本評価	<ul style="list-style-type: none"> •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)：不要 •機密性への影響(C)：部分的 •完全性への影響(I)：部分的 •可用性への影響(A)：部分的
CVSS v2 基本値	6.8 (レベルⅡ)

5.3 完全なログアウトについて

何らかの方法で有効なセッション ID を取得した攻撃者に悪用された場合、正規の利用者がログアウトしても成りすまし行為が継続される可能性がある現象が確認されております。弊社では本現象を制限事項として、公開をいたしております。詳細は以下の弊社ホームページにある「制限事項」をご覧ください。

<https://www.cybozu.com/jp/service/restrictions.html>

今後 cybozu.com の各サービスが利用するセッション情報を共通化し、シングルログアウトを可能とすることを予定いたしております。