

Garoon 脆弱性検査結果

1 概要

2016年2月03日から2016年2月05日に、サイバーディフェンス研究所様にて Garoon 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2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

2016年5月にリリースいたしました Garoon 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。

- 承認されると自動で予定が登録される、スケジュール連携機能(ワークフロー)
- 運用管理権限の委譲機能(掲示板)
- 全文検索の検索画面でカテゴリを検索する機能(掲示板)
- スレッドを別のスペースに移動できる機能(スペース)

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	各利用者にと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

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

2 件の脆弱性が検出されました。

脆弱性識別番号	CyVDB-1162
脆弱性タイプ	CWE-79 : XSS
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 • 必要な特権レベル(PR) : 高 • 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	4.8

脆弱性識別番号	CyVDB-1206
脆弱性タイプ	CWE-264 : 認可・権限・アクセス制御
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•必要な特権レベル(PR) : 低•ユーザー関与レベル(UI) : 不要•影響の想定範囲(Scope) : 変更なし•機密性への影響(C) : 低•完全性への影響(I) : なし•可用性への影響(A) : なし
CVSS v3 基本値	4.3