不具合情報公開サイト 脆弱性監査結果

1 概要

2020 年 5 月 20 日から 2020 年 5 月 22 日に、ゲヒルン株式会社様にて不具合情報公開サイト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 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 監査対象について

2020 年 6 月にリリースいたしました不具合情報公開サイトに関して、公開前に監査いただきました。監査対象の機能は以下の通りです。

- 検索機能
- フィードバック機能

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。

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

3 件の脆弱性が検出されました。

脆弱性識別番号	CyVDB-2672
脆弱性タイプ	CWE-79：Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
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

脆弱性識別番号	CyVDB-2674
脆弱性タイプ	CWE-352：Cross-Site Request Forgery (CSRF)
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)：変更なし •機密性への影響(C)：なし •完全性への影響(I)：低 •可用性への影響(A)：なし
CVSS v3 基本値	4.3

脆弱性識別番号	CyVDB-2675
脆弱性タイプ	CWE-352：Cross-Site Request Forgery (CSRF)
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)：変更なし •機密性への影響(C)：なし •完全性への影響(I)：低 •可用性への影響(A)：なし
CVSS v3 基本値	4.3