EC-CUBE4.2バグバウンティ ルールについて

0. はじめに

EC-CUBE4.2バグバウンティ(以下本バグバウンティ)は、EC-CUBE4.2や4.2対応のEC-CUBE公式プラグイン、及び指定されたプラグインに存在するバグや脆弱性を発見し改修することにより、EC-CUBE4.2のクオリティとセキュリティ向上を目的とするイベントです。

本イベントに基づきバグや脆弱性を発見し、報告・修正、及び実際に該当アプリケーションに取り込まれた際には、報告者へEC-CUBE4.2の品質向上にご協力いただいた謝礼として、報酬を贈呈いたします。

(報酬の詳細は決定次第発表いたします。)

1. 検証対象

本バグバウンティの検証対象となるのは、EC-CUBE4.2や4.2対応のEC-CUBE公式プラグイン、及び指定されたプラグインとなります。

検証対象や検証環境の詳細は以下ページをご覧ください。

https://www.ec-cube.net/user_data/event/bugbounty2022/eccube_bugbounty2022_check.pdf

各アプリケーションは最終更新分を対象といたします。

各アプリケーションの更新は、イベント期間中バグ修正がなされ、随時更新される可能性がございますので、アプリケーションが最新かどうかは、それぞれ該当アプリケーションの更新日時をご確認ください。

2.参加資格

以下の条件をすべて満たした方は、本バグバウンティに参加することができます。

報告時においてイルグルムグループ従業員でないこと

報告時においてイルグルムグループと業務委託契約、出向契約、派遣契約などの契約形態によりイルグルムグループの業務に従事していないこと

日本語でイーシーキューブ社の担当者とコミュニケーションできること

自身でバグバウンティに参加するための環境、機材を用意できること

3. 参加申込とバグ・脆弱性報告方法

本バグバウンティは、(株)イーシーキューブが運営しています。

本バグバウンティ参加には、参加フォームより登録をお願いします。

本バグバウンティにおける脆弱性ではないバグ報告やバグ修正報告はEC-CUBE GitHubにて受け付けます。また、脆弱性報告に関しては報告が一般公開されないよう、別途お問合せフォームにて受け付けます。通常バグか脆弱性の判断がつかない場合はお問合せフォームからご報告をお願いします。
いただいた脆弱性の情報は改修され該当アプリケーション(EC-CUBE本体及び各プラグイン)がリリースされるまで一般公開はされません。

本バグバウンティ参加フォーム：https://forms.gle/w5hy2yowvS3n5jnP9

バグ報告・バグ修正方法はこちら：https://www.ec-cube.net/committer/

脆弱性のご報告はこちらの問い合わせフォームへ：https://www.ec-cube.net/contact/

5.バグ・脆弱性の対応プロセス

5.1 バグの対応プロセス

報告者がバグ報告やバグ修正報告をEC-CUBE4.2 GitHubに登録した場合、以下のプロセスでバグの確認、アプリケーションへの取り込みを行います。

【バグ報告(Issue)】

・GitHubへバグ報告を行った場合、その内容がバグであるかどうかの確認を行います。
・バグであった場合は、issueに「バグ」ラベルを付与します。また、バグバウンティのポイントを同時に付与します。
・バグ修正がセットでなかった場合、本バグバウンティのどなたでもバグ修正を実施できます。

【バグ修正(Pull Request)】

・GitHubへバグ報告とバグ修正報告を同時に行うことができます。

・バグ報告のみのチケットに対し、バグ修正報告を行うことができます。
・バグ修正報告を行った場合は、(株)イーシーキューブでバグ修正方法や動作の確認を行います。
・正しくバグ修正されている場合は【バグ修正取り込み】が実施されます。
・バグ修正は、EC-CUBE4.2.0に必ず取り込まれるとは限りません。(EC-CUBE4.2.xでの取り込みになる可能性があります。)

【バグ認定・修正取り込み】

・バグ修正方法や動作確認完了後、対象のアプリケーションにバグ修正取り込みが行われます。
・バグ修正は、EC-CUBE4.2.0に必ず取り込まれるとは限りません。(EC-CUBE4.2.xでの取り込みになる可能性があります。)

【脆弱性報告】

・脆弱性報告は、EC-CUBEお問合せフォームから報告します。
・脆弱性の判断を(株)イーシーキューブで実施します。
・脆弱性であると判断された場合、報告者へ通知します。(本バグバウンティでの脆弱性報告者の方はIPAの報告等にもご協力いただきます。)
・脆弱性の危険度等に応じて、公開バージョン、公開時期を(株)イーシーキューブで判断します。
・脆弱性は該当アプリケーション(EC-CUBE本体及び各プラグイン)がリリースされるまで一般公開はされません。

【報酬】

・バグ報告・バグ修正・バグ修正取り込み・脆弱性報告それぞれに対応した点数を参加者に付与します。
・本バグバウンティ受付終了後、付与された点数を集計し順位を決定します。
・報酬は順位により決定します。
・報酬は、本バグバウンティ点数上位者には2022年9月に開催される、EC-CUBE4.2リリースパーティにて目録をお渡しし、その後、原則として振込にてお渡しします。

5.2 受付順序について

報告のあったバグ報告、バグ修正報告、脆弱性報告は、報告された順に受け付けます。

まったく同様の事象が先に報告されている場合は、後からの報告は点数が加算されませんのでご注意ください。また異なる事象であってもバグの根本原因が同様の場合は、後からの報告の点数が加算されない可能性がございますのでご注意ください。

5.4 対応順序について

原則として報告の早い順に確認を行いますが、バグや脆弱性の危険度、修正難易度や報告状況などにより確認順序が入れ替わることがあります。

6.バグ・脆弱性の点数に関して

報告されたバグや脆弱性は以下のルールで点数を付与します。

※情報が不十分で提示した期限内に有効な情報をいただけない場合は点数が付与されない可能性がございますのでご了承ください。

【バグ報告】

バグ報告に関わる点数は以下とします。

■Issue登録者の獲得できる点数

・バグ報告（Issue登録）：1点

・再現手順の記述：5点

・バグ認定：5点

バグの大小に関わらず同点数とします。

報告したバグが確認の結果バグであると認定された場合5点追加加点とします。

■Issue登録者以外の方が獲得できる点数

・Issue登録者以外の再現性確認報告：3点

【バグ修正】

バグ修正に関わる点数は以下とします。

また、バグ修正はIssue登録者以外の方でも登録が可能です。

■バグ修正者が取得できる点数

・バグ修正（Pull Request登録）：5点

・テストコード記述：5点

・バグ修正認定：10点

バグ修正の難易度に関わらず同点数とします。

報告したバグ修正が、正しい修正であると認定された場合10点追加加点とします。

【脆弱性報告】

脆弱性報告に関わる点数は以下とします。

■脆弱性報告者が獲得できる点数

・脆弱性報告(事象と再現手順含む)：10点

・脆弱性認定：40点

脆弱性報告や結果は各アプリケーションのリリースまで内容が公開されることはありません。

報告されたものが、脆弱性と認定された場合は40点追加点とします。

脆弱性と認定されない場合(通常の不具合と認定、攻撃が不可能な場合、仕様であった場合等)もございますので、ご了承ください。

【その他セキュリティに関する提案等の加点】

バグや脆弱性ではなく、セキュリティに関する修正や機能提案をいただいた場合も、点数を加点できる可能性があります。

GitHubのissueにご提案をお願いします。内容を判断し、任意の点数を付与いたします。

7. 報酬

7.1 報酬について

報酬は、バグバウンティで獲得した点数総数の順位により決定します。

順位に応じた報酬金額は以下の通りです。

1位：42万円

2位：30万円

3位：21.7万円

4位～8位：5万円

その他の報酬、副賞に関しては決まり次第発表いたします。

7.2 報酬獲得ルールの補足

項目	概要	ルール
1	確認結果により複数のバグが認定された	確認結果により1報告につき複数のバグが認定された場合、それらの数に応じた点数を獲得できます。
2	同一要因のバグが報告された	同一アプリケーションで、同一要因のバグや脆弱性が報告された場合、先に報告されたバグや脆弱性を認定します。認定された報告者のみ点数を獲得できます。
3	既知のバグや脆弱性が報告された	既に公開されているバグや脆弱性を報告いただいた場合、点数を獲得できません。
4	動作環境外のバグや脆弱性が報告された	動作環境外で再現するバグや脆弱性を報告いただいた場合、バグや脆弱性と認定されず点数が獲得できません。動作環境についてはEC-CUBE4.2動作環境を確認してください。

7.3 税金について

報酬を獲得した報告者は、各国の制度に基づき申告が必要になる場合があります。

国や税制度は異なるため、制度に関してはご自身で調査し、対応してください。

なお、支払調書は確定申告書に添付する必要がないため、発行しません。

8.著作権の取り扱い

バグ修正に伴って発生したコードやその他のデータ・文章には、githubのプロジェクトページ(https://github.com/EC-CUBE/ec-cube)に記載の「EC-CUBEのコピーライトポリシー」が適用されます。同ポリシーの適用により、データ・文章の当該著作財産権（著作権法第２７・２８条の権利を含みます）が報告者から(株)イーシーキューブに移転する他、その他の注意事項があります。本バグバウンティへの参加にあたっては、同ポリシーをよくご理解の上、ご承諾いただく必要があります。

9.本バグバウンティルールの変更

本バグバウンティルールは、事前に公表することなく、変更を行うことがあります。 本ルールブックの重要部分に変更があった場合は、本バグバウンティ参加者に対しその内容を通知します。

2022年7月13日 制定
2022年8月16日 更新（報酬のお渡し方法、報酬金額）