ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系）の脆弱性について

公開日　2019 年 10 月 2 日
最終更新日　2019 年 10 月 9 日

時下、御社ますますご清栄のこととお慶び申し上げます。
また、日頃より「ルミーズ」のご愛顧を賜りまして、心より御礼申し上げます。

さて、弊社から提供しております、EC-CUBE2 系の決済モジュール『ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系)』におきまして複数の脆弱性があることが判明しました。
加盟店の皆様におかれましては、大変ご迷惑をお掛けしておりますことを深くお詫び申し上げます。
詳細情報につきまして、以下の通りご報告を申し上げます。

■概要

EC-CUBE2 系の決済モジュール『ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系)』のバージョン 3.0.12 以前に情報漏洩及びクロスサイトスクリプティングの脆弱性の存在が判明しました。
この脆弱性を悪用された場合、悪意ある第三者の攻撃により、情報漏洩等の危険性があります。
この問題の影響を受けるルミーズ決済モジュール（2.11 系・2.12 系・2.13 系）のバージョンを以下に示しますので、以下の修正プログラムを適用してください。

■該当モジュールの確認方法

モジュール名称：ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系）
該当バージョン：バージョン 3.0.12 以前の全てのバージョン

使用しているバージョン番号の確認方法は以下の通りです。

・2.11 系の場合
(1) 「EC-CUBE 管理画面＞オーナーズストア」をクリック
(2) 「購入商品一覧を取得する」ボタンをクリック
(3) 表示されたモジュール一覧の、「ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系)」の導入バージョンを確認

・2.12 系、2.13 系の場合
(1)「 EC-CUBE 管理画面＞オーナーズストア＞モジュール管理」をクリック
(2) 「モジュール一覧を取得」ボタンをクリック
(3) 表示されたモジュール一覧の、「ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系)」の導入バージョンを確認

■脆弱性の説明

ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系）で使用される一部機能を利用して、特定の情報の抽出及び任意のスクリプトを実行される脆弱性が存在します。

攻撃者および被害者の条件については以下の通りです。

・攻撃者の条件

管理者、一般ユーザのログイン有無にかかわらず、誰でも攻撃可能。

・被害者の条件

当該 EC-CUBE 利用サイトで会員登録の有無に関係なく注文を行ったことがあるユーザ全てが対象。

また、ルミーズ決済モジュールで提供する決済方法（クレジットカード決済・マルチ決済）に限らず、全ての決済方法が対象です。

■脆弱性がもたらす脅威

本モジュールをインストールしている場合、攻撃が成功すると悪意のある第三者によって、お客様の個人情報が抜き出される可能性、及び任意のスクリプトを実行される可能性があります。

■対策方法

・修正方法：モジュールのバージョンアップ

バージョン 3.0.13 以降のモジュールにバージョンアップを行うことで、本件の脆弱性は修正されます。

アップデート方法は、EC-CUBE 管理画面のモジュール一覧より、ルミーズ決済モジュール（2.11 系・2.12 系・2.13 系）の「アップデート」もしくは「ダウンロード」のリンクをクリックしていただく事でアップデートを行うことができます。

※カスタマイズ等によりモジュールのアップデートが難しい場合、弊社テクニカルデスクまでご相談ください。

■関連情報

JVN#59436681
EC-CUBE 用モジュール「ルミーズ決済モジュール(2.11 系・2.12 系・2.13 系)」における複数の脆弱性
https://jvn.jp/jp/JVN59436681/index.html

■謝辞

本情報のご提供様および関係各位には、この場をお借りして、厚く御礼申し上げます。

■更新履歴

2019 年 10 月 2 日 この脆弱性情報について加盟店様へ公開しました。
2019 年 10 月 7 日 この脆弱性情報について一般公開をしました。
「■関連情報」を追記しました。
2019 年 10 月 9 日 「■対策方法」にモジュールアップデート方法について、追記を行いました。

■連絡先

「ルミーズ」テクニカルデスク ： tech@remise.jp
TEL:(0267)26-5318 / FAX:(0267)26-5316
（平日 9:00 - 19:00）