EC-CUBE 2系における複数の脆弱性 (JVN#75444925)

更新履歴

2021/11/11 17:00
　　「脆弱性の概要」に、JVNからの公表内容情報へのリンクを追加
2021/11/11 11:00
　　初版公開

EC-CUBE 2系における2件の脆弱性のお知らせ

EC-CUBE 2系に2件の脆弱性(緊急度 中：1件、緊急度 低：1件)があることが判明いたしました。

脆弱性そのものは、修正ファイルの反映によりすぐに解決するものです。以下のいずれかの方法により、ご対応をお願いいたします。

- 修正方法1: EC-CUBEのバージョンアップを行う場合
- 修正方法2: 修正差分を確認して適宜反映する場合

皆様にはお手数おかけし誠に申し訳ございません。
本脆弱性における被害報告は現時点でございませんが、できるだけ速やかにご対応をお願いいたします。

脆弱性の概要

1. 管理画面におけるCSRF

危険度:
中

不具合が存在するEC-CUBEのバージョン:
2.11.0 〜 2.17.1

詳細:
管理画面にログインした状態の管理者権限を持つユーザが、細工されたページに誘導され特定のURLにアクセスした場合、意図せず管理ユーザを削除される CSRF脆弱性。

---

2. 認可制御の不備

危険度:
低

不具合が存在するEC-CUBEのバージョン:
2.11.2 〜 2.17.1

詳細:
店舗オーナー権限を持つユーザによって、本来操作権限のないシステム設定の変更が可能となる認可制御の不備。
なお、管理画面の「システム設定」→「マスタデータ管理」より、mtb_permission の ID を管理画面URLと同じディレクトリ名に変更することで回避可能です。

例:
管理画面URLが `example.com/example-admin/` の場合、マスタデータ管理の mtb_permission の ID `/admin/system/index.php` を、`/example-admin/system/index.php` に変更する (その他のIDも同様に、ディレクトリ名部分を変更する)

JVNからの公表内容 (2021/11/11公開)

JVN#75444925: EC-CUBE 2系における複数の脆弱性

修正方法1: EC-CUBEのバージョンアップを行う場合

EC-CUBE 2.17.2以降の最新版にバージョンアップしていただくことで、本件の脆弱性は修正されます。

公式サイトのダウンロードページから最新バージョンをダウンロードしてご利用ください。

修正方法2: 修正差分を確認して適宜反映する場合

EC-CUBE本体のソースコードをカスタマイズされている方向けです。
下記のコード差分情報を参照して頂き、必要な箇所に修正を反映してください。

サポート対象バージョン

- **EC-CUBE 2.17.1**
- **EC-CUBE 2.13.5**

(旧バージョンのEC-CUBEをお使いの方は、最新バージョンへのアップデートを推奨いたします)

修正対象ファイル

以下の3ファイルとなります。

- /data/class/SC_Session.php
- /data/class/pages/admin/system/LC_Page_Admin_System_Delete.php
- /html/user_data/packages/admin/js/eccube.admin.js

修正差分

EC-CUBE 2.17.1 / 2.13.5 とも、同一内容となります。

data/class/SC_Session.php CHANGED

```
@@ -65,7 +65,7 @@ class SC_Session
         }
     }
     /* 認証成功の判定 */
-    public function IsSuccess()
+    public function IsSuccess($admin_dir = ADMIN_DIR)
     {
         if ($this->cert == CERT_STRING) {
             $script_path = realpath($_SERVER['SCRIPT_FILENAME']);
@@ -75,7 +75,15 @@ class SC_Session
             $arrPERMISSION = $masterData->getMasterData('mtb_permission');

             foreach ($arrPERMISSION as $path => $auth) {
-                $permission_path = realpath(HTML_REALDIR . $path);
+                if (stripos($path, '/admin/') === 0) {
+                    // path が /admin で始まる場合は /admin を削除
+                    $path = str_replace('/admin', '', $path);
+                } elseif (stripos($path, '/'.$admin_dir) === 0) {
+                    // path が /ADMIN_DIR で始まる場合は /ADMIN_DIR を削除
+                    $path = str_replace('/'.$admin_dir, '', $path);
+                }
+                $permission_path = realpath(HTML_REALDIR.$admin_dir.$path);

                 $arrPermissionPath = explode('/', str_replace('\\', '/', $permission_path));
                 $arrDiff = array_diff_assoc($arrScriptPath, $arrPermissionPath);
                 // 一致した場合は、権限チェックを行う
```

data/class/pages/admin/system/LC_Page_Admin_System_Delete.php CHANGED

```
@@ -60,6 +60,10 @@ class LC_Page_Admin_System_Delete extends LC_Page_Admin_Ex
      */
     public function action()
     {
+        if ($this->getMode() !== 'delete') {
+            SC_Utils_Ex::sfDispError(INVALID_MOVE_ERRORR);
+            SC_Response_Ex::actionExit();
+        }
         $objFormParam = new SC_FormParam_Ex;

         // パラメーターの初期化
```

html/user_data/packages/admin/js/eccube.admin.js CHANGED

```
@@ -31,7 +31,8 @@

     //指定されたidの削除を行うページを実行する。
     eccube.deleteMember = function(id, pageno, lastAdminFlag) {
-        var url = "./delete.php?id=" + id + "&pageno=" + pageno;
+        var transactionid = $('input[name=transactionid]').val();
+        var url = "./delete.php?id=" + id + "&pageno=" + pageno + "&mode=delete&transactionid=" + transacti
         var message = lastAdminFlag ?
         '警告: 管理者がいなくなってしまいますと、システム設定などの操作が行えなくりますが宜しいでしょうか'
         : '登録内容を削除しても宜しいでしょうか';
```

問い合わせ先

本脆弱性に関するお問合せ：

EC-CUBE 運営チーム
MAIL: support@ec-cube.net