DefenseCode

DefenseCode ThunderScan SAST Advisory

# WordPress Easy Modal Plugin
# Multiple Security Vulnerabilities

| WordPress Easy Modal Plugin –Multiple Security Vulnerabilities | |
|---|---|
| Advisory ID: | **DC-2017-01-007** |
| Software: | **WordPress Easy Modal plugin** |
| Software Language: | **PHP** |
| Version: | **2.0.17 and below** |
| Vendor Status: | **Vendor contacted, update released** |
| Release Date: | **2017/08/07** |
| Risk: | **Medium** |

## 1. General Overview

During the security audit of Easy Modal plugin for WordPress CMS, multiple vulnerabilities were discovered using DefenseCode ThunderScan application source code security analysis platform.

More information about ThunderScan is available at URL:
http://www.defensecode.com

## 2. Software Overview

According to the plugin developers, Easy Modal is the #1 WordPress Popup Plugin. It's advertised as "Make glorious & powerful popups and market your content like never before - all in minutes!".

According to wordpress.org, it has more than 20,000 active installs.

Homepage:
http://wordpress.org/extend/plugins/easy-modal/
https://easy-modal.com

## 3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerabilities in Easy Modal WordPress plugin.

The easiest way to reproduce the vulnerability is to visit the provided URL while being logged in as administrator or another user that is authorized to access the plugin settings page. Users that do not have full administrative privileges could abuse the database access the vulnerability provides to either escalate their privileges or obtain and modify database contents they were not supposed to be able to.

The nonce token is required as the URL parameter. Token value is not unique for each request, nor per each URL, so if the attacker manages to obtain a valid token value, the module could be exposed to attack vectors such as Cross Site request forgery (CSRF).

### 3.1. SQL injection

| | |
|---|---|
| Vulnerable Function: | **$wpdb->query()** |
| Vulnerable Variables: | **$_GET['id'], $_GET['ids'], $_GET['modal']** |

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=easy-
modal&action=delete&id%5B0%5D=4%20AND%20SLEEP(5)&easy-modal_nonce=xxx
```

File: easy-modal\classes\controller\admin\modals.php

```
93      $ids = is_array($_GET['id']) ? $_GET['id'] : array($_GET['id']);
...
97      $ids = $_GET['ids'];
...
101     $ids = $_GET['modal'];
...
110     $wpdb->query("UPDATE {$wpdb->prefix}em_modals SET is_trash = 1 WHERE id IN
("implode(',', $ids).")");
```

### 3.2. SQL injection

| | |
|---|---|
| Vulnerable Function: | **$wpdb->query()** |
| Vulnerable Variables: | **$_GET['id'], $_GET['ids'], $_GET['modal']** |

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?easy-
modal_nonce=xxx&_wp_http_referer=%2Fvulnerablesite.com%2Fwp-admin%2Fadmin.php%3Fpage%3Deasy-
modal%26status%3Dtrash&page=easy-modal&action=untrash&paged=1&id[]=2)%20AND%20SLEEP(10)--
%20ZpVQ&action2=-1
```

File: easy-modal\classes\controller\admin\modals.php

```
123     $ids = is_array($_GET['id']) ? $_GET['id'] : array($_GET['id']);
...
127     $ids = $_GET['ids'];
...
131     $ids = $_GET['modal'];
...
140     $wpdb->query("UPDATE {$wpdb->prefix}em_modals SET is_trash = 0 WHERE id IN ($ids)");
```

## 4. Solution

Vendor resolved the security issues after we reported the vulnerability. All users are strongly advised to update WordPress Easy Modal plugin to the latest available version.

## 5. Credits

Discovered with DefenseCode ThunderScan source code security analyzer by Neven Biruski.

## 6. Disclosure Timeline

| | |
|---|---|
| 2017/04/04 | **Vendor contacted** |
| 2017/04/06 | **Vendor responded** |
| 2017/04/13 | **Update released** |
| 2017/08/07 | **Advisory released to the public** |

## 7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

**Subscribe for free software trial on our website** http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/