DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Ultimate Form Builder Lite Plugin Multiple Vulnerabilities (XSS and SQLi)

WordPress Ultimate Form Builder Lite Plugin – Multiple Vulnerabilities (XSS and SQLi)	
Advisory ID:	**DC-2018-05-009**
Software:	**WordPress Ultimate Form Builder Lite plugin**
Software Language:	**PHP**
Version:	**1.3.7 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2018/06/12**
Risk:	**Medium**

1. General Overview

During the security audit of Ultimate Form Builder Lite 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, Ultimate Form Builder Lite is a free WordPress Plugin which allows you to create various contact forms with drag and drop form builder. Its fun because – you can create, customize and build the beautiful forms for your site on your own, receive contact email on any desired email address and store the form entries in your database which can be exported to CSV for your use via plugin's backend.

According to wordpress.org, it has more than 40,000 active installs.

Homepage:
https://wordpress.org/plugins/ultimate-form-builder-lite/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting and SQL injection vulnerabilities in Ultimate Form Builder Lite WordPress plugin.

The Cross-Site Scripting vulnerability can enable the attacker to construct the URL that contains malicious JavaScript code. If the administrator of the site makes a request to such an URL, the attacker's code will be executed, with unrestricted access to the WordPress site in question. The attacker can entice the administrator to visit the URL in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum.

The easiest way to reproduce the SQL injection 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.

3.1 Cross-Site Scripting

Vulnerable Function:	**echo()**
Vulnerable Variable:	**$_GET['form_id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=ufbl&action=edit-
form&form_id=1"><script>alert(42)</script>
```

File: ultimate-form-builder-lite/inc/views/backend/form-builder.php

```
10 <div class="ufbl-shortcode-display-wrap">Shortcode: <input type="text"
onfocus="this.select();" readonly="readonly" value="[ufbl form_id=&amp;quot;<?php echo
$_GET['form_id']?>&amp;quot;]" class="shortcode-in-list-table wp-ui-text-highlight code"></div>
```

3.2 SQL injection

Vulnerable Function:	**$wpdb->get_row()**
Vulnerable Variable:	**$_POST['entry_id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin-ajax.php
```

Vulnerable POST body:

```
entry_id=1&_wpnonce=xxx&action=ufbl_get_entry_detail_action
```

File: ultimate-form-builder-lite/ultimate-form-builder-lite.php

```
369 $entry_id = sanitize_text_field( $_POST['entry_id'] );
...
370 $entry_row = $this->model->get_entry_detail( $entry_id );
```

File: ultimate-form-builder-lite\classes\ufbl-model.php

```
243 public static function get_entry_detail( $entry_id ) {
...
248 $entry_row = $wpdb->get_row( "SELECT * FROM $entry_table INNER JOIN $form_table ON
$entry_table.form_id = $form_table.form_id WHERE $entry_table.entry_id = $entry_id",
'ARRAY_A' );
```

4. Solution

After the vulnerabilities were reported the vendor resolved the security issues. All users are strongly advised to update WordPress Ultimate Form Builder Lite plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2018/06/01	**Vulnerabilities discovered**
2018/06/06	**Vendor contacted**
2018/06/08	**Vendor responded**
2018/06/12	**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/