
## DefenseCode ThunderScan SAST Advisory

# Ultimate Form Builder

# Cross-Site Scripting (XSS) Vulnerability

| Ultimate Form Builder - Cross-Site Scripting (XSS) Vulnerability | |
|---|---|
| Advisory ID: | **DC-2017-01-027** |
| Software: | **Ultimate Form Builder WordPress plugin** |
| Software Language: | **PHP** |
| Version: | **Various** |
| Vendor Status: | **Vendor contacted** |
| Release Date: | **20170419** |
| Risk: | **Medium** |

## 1. General Overview

During the security audit, security vulnerability was discovered in Ultimate Form Builder WordPress plugin using DefenseCode ThunderScan web application source code security analysis platform.

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

## 2. Software Overview

According the plugin developers, Ultimate Form Builder allows you to create various contact forms with drag and drop form builder. It's 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. It has more than 60,000 downloads on wordpress.org.

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

## 3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross Site Scripting vulnerability in Ultimate Form Builder 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.

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, or embedding it as an IMG tag source in another web page administrator will visit, causing the administrator's browser to request the URL automatically - due to missing nonce token the vulnerability is directly exposed to Cross site request forgery, (CSRF) attacks.

The JavaScript code could enable the attacker to make requests with administrator privileges, or grab the session ID and be able to interact with the administrative pages through his own browser.

| 3.1 Cross-Site Scripting | |
|---|---|
| Function: | **Echo** |
| Variable: | **$_GET['ufbl_form_id']** |

Sample URL:

```
http://vulnerablesite.com/?ufbl_form_preview=true&ufbl_form_id=1"><script>alert(42)</script>
```

File: ultimate-form-builder-lite\inc\views\frontend\preview-form.php

```
19    <span class="ufb-preview-subtitle"><a href="<?php echo
admin_url('admin.php?page=ufbl&action=edit-form&form_id='.$_GET['ufbl_form_id']);?>"><?php
_e('Edit Form','ultimate-form-builder-lite');?></a></span>
```

## 4. Solution

Vendor did not respond to our repeated attempts to send this advisory. All users are strongly advised to update WordPress AccessPress Social Icons plugin to the latest available version.

## 5. Credits

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

## 6. Disclosure Timeline

| | |
|---|---|
| 03/24/2017 | **Vendor contacted** |
| 04/12/2017 | **Vendor contacted** |
| 04/13/2017 | **Vendor contacted** |
| 04/19/2017 | **Still no response. 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/