DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress PressForward Plugin Security Vulnerability

WordPress PressForward Plugin –Security Vulnerability	
Advisory ID:	**DC-2017-05-007**
Software:	**WordPress PressForward plugin**
Software Language:	**PHP**
Version:	**4.3.0 and below**
Vendor Status:	**Vendor contacted**
Release Date:	**2017/08/07**
Risk:	**Medium**

1. General Overview

During the security audit of PressForward plugin for WordPress CMS, security vulnerability was 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, PressForward provides an editorial workflow for content aggregation and curation within the WordPress dashboard. It is designed for bloggers and editorial teams who wish to collect, discuss, and share content from a variety of sources on the open web.

It's users and partners include numerous universities, centers, laboratories, colleges and various kinds of organizations.

Homepage:

https://wordpress.org/plugins/pressforward/
http://pressforward.org/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting vulnerability in PressForward 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 vulnerability was tested using Apache web server.

3.1 Cross-Site Scripting	
Vulnerable Function:	**Echo**
Vulnerable Variable:	**$_SERVER['PHP_SELF']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php/%22%3E%3Cimg%20src=x%20onerror=alert(42)%3E/?page=pf-menu#ready
```

File: pressforward-master\Core\Admin\PFTemplater.php

```
<form id="feeds-search" method="post" action="<?php echo basename( $_SERVER['PHP_SELF'] ) . '?' . $_SERVER['QUERY_STRING'] . '&action=post'; ?>">
```

4. Solution

Vendor should resolve the security issues in next release. All users are strongly advised to update WordPress PressForward plugin to the latest available version as soon as the vendor releases an update that fixes the vulnerability.

5. Credits

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

6. Disclosure Timeline

2017/05/31	**Vendor contacted**
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/