

Multiple Vulnerabilities Patched in Responsive Menu Plugin



Chloe Chamberland

February 10, 2021

Multiple Vulnerabilities Patched in Responsive Menu Plugin

On December 17, 2020, our Threat Intelligence team responsibly disclosed three vulnerabilities in [Responsive Menu](#), a WordPress plugin installed on over 100,000 sites. The first flaw made it possible for authenticated attackers with low-level permissions to upload arbitrary files and ultimately achieve remote code execution. The remaining two flaws made it possible for attackers to forge requests that would modify the settings of the plugin and again upload arbitrary files that could lead to remote code execution. All three vulnerabilities could lead to a site takeover, which could have consequences including backdoors, spam injections, malicious redirects, and other malicious activities.

We initially attempted to reach out to the team at Responsive Menu through their parent company ExpressTech on December 17, 2020. After receiving no response for a few weeks, we tried reaching out through the contact form on the Responsive Menu site on January 4, 2021, and again received no response after a week. At that point we felt it best to escalate the issue to the WordPress Plugins team on January 10, 2021. We received a response from the plugins team and the plugin's founder thereafter on January 11, 2021. Once contact was established, they were very quick to resolve the issues and released a patch on January 19, 2021.

All three patched flaws are considered medium and critical severity vulnerabilities. Therefore, we highly recommend updating to the patched version, 4.0.4, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on December 17, 2020. Sites still using the free version of Wordfence received the same protection on January 16, 2021.

Description: Authenticated Arbitrary File Upload
Affected Plugin: Responsive Menu
Plugin Slug: responsive-menu
Affected Versions: <= 4.0.0 – 4.0.3
CVE ID: [CVE-2021-24160](#)
CVSS Score: 9.9 (Critical)
CVSS Vector: [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/H/I/H/A/H](#)
Fully Patched Version: 4.0.4

Responsive Menu is a plugin designed to create highly responsive and customizable menus for WordPress sites. It contains several features that allow users to easily create a beautiful menu interface with different colors and designs. As part of the plugin's functionality, site owners have the option to import themes from zip files that can either be custom creations or downloaded from the Responsive Menu site. In order to provide this functionality, the plugin registered an `admin_post` action, `admin_post_rmp_upload_theme_file`, tied to the function `rmp_upload_theme`.

```
53 | add_action('admin_post_rmp_upload_theme_file', array( $this, 'rmp_upload_theme' ) );
```

The `rmp_upload_theme` function takes a zip file supplied by the `admin_post` request and extracts its contents to the `/rmp-menu/themes/` directory.

```
311 | public function rmp_upload_theme() {  
312 |     status_header(200);  
313 |     $theme = $this->file['file'];  
314 |     WP_Filesystem();  
315 |     $upload_dir = wp_upload_dir()['basedir'] . '/rmp-menu/themes/';  
316 |     $unzip_file = unzip_file($theme, $upload_dir);  
317 |     if ( !is_wp_error($unzip_file) ) {  
318 |         $status = [ 'danger' => $unzip_file->get_error_message() ];  
319 |     } else {  
320 |         $status = [ 'success' => 'Theme Imported Successfully.' ];  
321 |     }  
322 |     return $status;  
323 | }
```

Unfortunately, there were no capability checks on this function, and due to the fact that it used `admin_post`, any user logged into a vulnerable WordPress site could execute this action to trigger the file upload and zip extraction. This included subscribers and other low level users, making sites with open registration particularly vulnerable. The `admin_post` action does not check to see whether a user is an administrator, but rather if the user is sending a request to the administrative page `/wp-admin/admin-post.php` while authenticated.

A subscriber could upload zip archives containing malicious PHP files that would get extracted to the `/rmp-menu/themes/` directory. These files could then be accessed via the front end of the site to trigger remote code execution and ultimately allow an attacker to execute commands to further infect a WordPress site.

In addition, there were no nonce checks on this function making it vulnerable to Cross-Site Request Forgery attempts as well.

This feature was introduced in version 4.0.0 of the plugin, therefore, only site running versions 4.0.0 – 4.0.3 of this plugin are considered vulnerable.

Description: Cross Site Request Forgery to Arbitrary File Upload
Affected Plugin: Responsive Menu
Plugin Slug: responsive-menu
Affected Versions: <= 4.0.3
CVE ID: [CVE-2021-24161](#)
CVSS Score: 8.8 (High)
CVSS Vector: [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I/H/A/H](#)
Fully Patched Version: 4.0.4

Prior to the major overhaul of the plugin in version 4.0.0, the theme import function was integrated within the settings area instead of using standalone functionality. The plugin received a POST request with the `responsive-menu-import-theme` parameter and file contents in the `responsive-menu-import-theme-file` parameter on the responsive-menu page.

```

46 | elseif(isset($_POST['responsive-menu-import-theme'])):
47 |     $file = $_FILES['responsive-menu-import-theme-file'];

```

If the `responsive-menu-import-theme` parameter was sent in a request, it triggered the `import_theme` function to start a theme import. This involved uploading and extracting the files from the supplied zip archive to the `/responsive-menu-themes` folder.

```

141 | public function import_theme($theme) {
142 |     if($theme) {
143 |         WP_Filesystem();
144 |         $upload_folder = wp_upload_dir()['basedir'] . '/responsive-menu-themes';
145 |         $upload_folder = $upload_folder;
146 |         $upload_dir = wp_upload_dir();
147 |         $upload_dir = $upload_dir;
148 |         if(is_wp_error($upload_dir)) {
149 |             $alert = ['danger' => $upload_dir->get_error_message()];
150 |         } else {
151 |             $alert = ['success' => 'Responsive Menu Theme Imported Successfully.'];
152 |         }

```

Though there was a permission check on this functionality that made it so that only administrators could trigger a theme import, there were no nonce checks to verify that a request came from a currently authenticated administrator's session. This meant that attackers could craft a request and trick an administrator into uploading a zip archive containing malicious PHP files. The attacker could then access those files to achieve remote code execution and further infect the targeted site.

Since this plugin underwent a major overhaul, this is considered a legacy feature. Only sites running versions older than 4.0.0 or running in legacy mode on versions 4.0.0 – 4.0.3 are considered vulnerable.

Description: Cross Site Request Forgery to Setting Modification
Affected Plugin: Responsive Menu
Plugin Slug: responsive-menu
Affected Versions: <= 4.0.3
CVE ID: CVE-2021-24162
CVSS Score: 5.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/L:L/A:L
 Fully Patched Version: 4.0.4

In addition to the theme import functionality, the plugin contained the ability to import new settings. The plugin checks for a POST request with the `responsive-menu-import` parameter and file contents in the `responsive-menu-import-file` parameter on the responsive-menu page.

```

40 | elseif(isset($_POST['responsive-menu-import'])):
41 |     $file = $_FILES['responsive-menu-import-file'];
42 |     $file_options = isset($_POST['tmp_name']) ? (array) json_decode(file_get_contents($file['tmp_name'])) : null;
43 |     echo $controller->import($file_options);

```

If the `responsive-menu-import-file` parameter was sent in a request, it would trigger the `import` function to start a settings import. This would then trigger the `updateOptions` function to update any of the options set for the plugin stored in the `responsive_menu` table.

```

269 | public function import($imported_options) {
270 |     $errors = [];
271 |     if(empty($imported_options)) {
272 |         $validator = new Validator();
273 |         if($validator->validate($imported_options)) {
274 |             try {
275 |                 $imported_options['button_click_trigger'];
276 |                 $options = $this->manager->updateOptions($imported_options);
277 |                 $task = new UpdateOptionsTask();
278 |                 $task->run($options, $this->view);
279 |                 $alert = ['success' => 'Responsive Menu Options Imported Successfully.'];
280 |             } catch (Exception $e) {

```

Again, although there was a permission check on this functionality restricting settings import to administrators, there were no nonce checks to verify that a request came from a currently authenticated administrator's session. This meant that attackers could craft a request and trick an administrator into importing all new settings. These settings could be modified to include malicious JavaScript, therefore allowing an attacker to inject payloads that could aid in further infection of the site.

Since this plugin underwent a major overhaul, this is considered a legacy feature. Only sites running versions older than 4.0.0 or running in legacy mode on versions 4.0.0 – 4.0.3 are considered vulnerable.

Disclosure Timeline

- December 17, 2020 – Conclusion of the plugin analysis that led to the discovery of the three vulnerabilities. We develop firewall rules to protect Wordfence customers and release them to Wordfence Premium users. We make our initial contact attempt via the ExpressTech.io contact form.
- January 4, 2021 – We make a second contact attempt, this time via the contact form on the Responsive Menu website.
- January 10, 2021 – We escalate the issue to the WordPress plugins team and provide full details at the time of reporting.
- January 11, 2021 – We receive a response from the WordPress plugins team and the founder of Responsive Menu. They verify that they will begin working on a fix.
- January 15, 2021 – Responsive Menu provides us with a copy of the intended patch to test. We verify it is sufficient and request additional security enhancements to be added.
- January 16, 2021 – Free Wordfence users receive firewall rules.
- January 18, 2021 – A patched version of the plugin is released as version 4.0.4. We verify again that the vulnerabilities have been patched.

Conclusion

In today's post, we detailed three flaws in the Responsive Menu plugin that granted attackers the ability to achieve remote code execution through arbitrary file uploads and to change settings. These flaws have been fully patched in version 4.0.4. We recommend that users immediately update to the latest version available, which is version 4.0.4 at the time of this publication.

Wordfence Premium users received firewall rules protecting against this vulnerability on December 17, 2020, while those still using the free version of Wordfence received the same protection on January 16, 2021.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as these are considered critical severity issues that can result in remote code execution.


Note: We have requested that the plugin's owner add further security hardening to the import of zip files. Though we received confirmation from the plugin owner that they would work on implementing this, it has been nearly a month with no visible progress on this request. Given the severity of the vulnerabilities already patched, we are publishing this advisement now so that site owners can update and protect their sites. We consider the remaining issue of significantly lower impact, as it would only affect very rare WordPress installations. We anticipate that they will soon resolve this issue, and we will update this post when completed.

Did you enjoy this post? Share it!

Comments

5 Comments

Craig Paterson *

 February 10, 2021
8:41 am



Chloe Chamberland *

February 10, 2021
2:29 pm

Hi Craig,

This does affect both the PRO and free versions of this plugin. These issues have been resolved in the same version (4.0.4) for both.



Craig Paterson *

February 11, 2021
8:42 am

Hi Chloe, thanks for that, but the latest available Pro version from their website is responsive-menu-pro-3.1.30



Chloe Chamberland *

February 15, 2021
12:29 pm

Hi Craig,

I was able to install 4.0.4 directly from their site for the PRO version, however, that was during a new sign-up. I recommend reaching out directly to their support team to see why that may be the case for you.



suraj singh *

February 24, 2021
2:17 am

Hello Guys

The responsive menu team has fixed all the vulnerabilities on all the versions include free.
If anyone still using the v3.x version and not updated for a long time and want to continue with that then please reach out to the support team.

They will provide you an updated one.

Breaking WordPress Security Research in your inbox as it happens.

☐ By checking this box I agree to the terms of service and privacy policy.*

[SIGN UP](#)

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

[Terms of Service](#)

[Privacy Policy](#)

[CCPA Privacy Notice](#)



Products

[Wordfence Free](#)
[Wordfence Premium](#)
[Wordfence Care](#)
[Wordfence Response](#)
[Wordfence Central](#)

Support

[Documentation](#)
[Learning Center](#)
[Free Support](#)
[Premium Support](#)

News

[Blog](#)
[In The News](#)
[Vulnerability Advisories](#)

About

[About Wordfence](#)
[Careers](#)
[Contact](#)
[Security](#)
[CVE Request Form](#)

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

☐ By checking this box I agree to the [terms of service](#) and [privacy policy](#).*

[SIGN UP](#)

© 2012-2022 Defiant Inc. All Rights Reserved