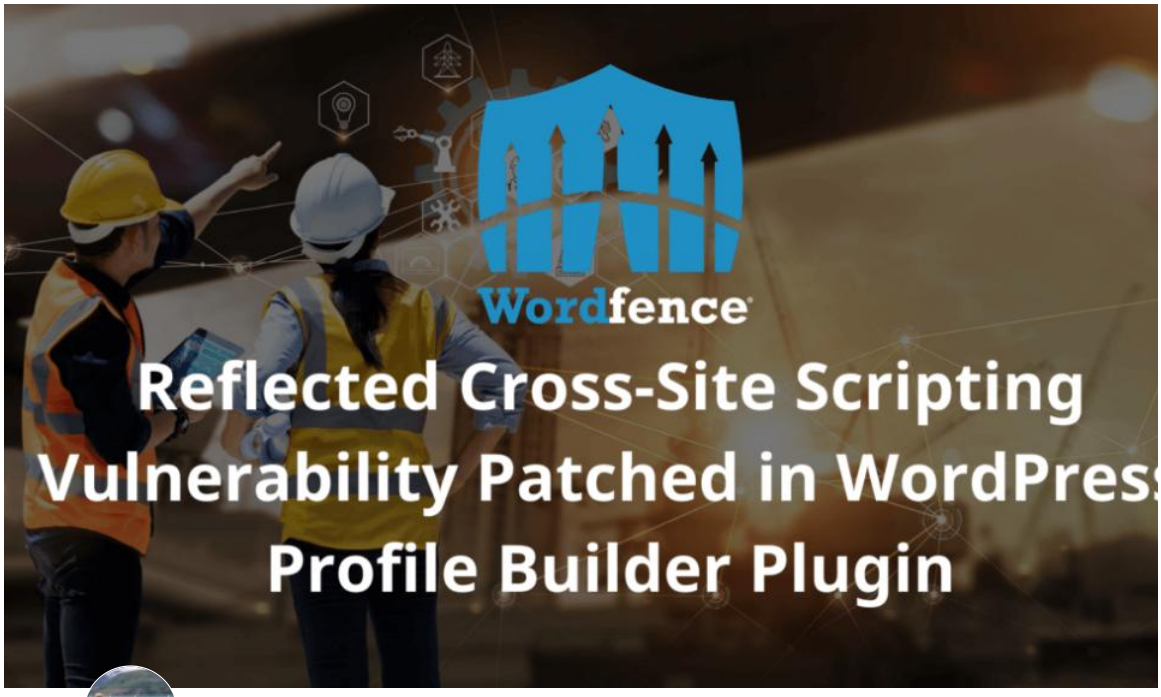
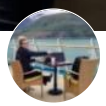




Chloe Chamberland

February 17, 2022

Reflected Cross-Site Scripting Vulnerability Patched in WordPress Profile Builder Plugin

On January 4, 2022 the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerability we discovered in "Profile Builder – User Profile & User Registration Forms", a WordPress plugin that is installed on over 50,000 WordPress websites. This vulnerability makes it possible for an unauthenticated attacker to craft a request that contains malicious JavaScript. If the attacker is able to trick a site administrator or user into performing an action, the malicious JavaScript executes, making it possible for the attacker to create new admin use redirect victims, or engage in other harmful attacks.

All Wordfence users, including users of our Free, Premium, Care, and Response products are protected from exploits targeting this vulnerability thanks to the Wordfence Firewall's built-in Cross-Site Scripting (XSS) protection.

We sent the full disclosure details to the developer on January 6, 2022 after the vendor confirmed the inbox for handl the discussion. They were quick to acknowledge the report and released a fix on January 10, 2022.

We strongly recommend ensuring that your site has been updated to the latest patched version of "Profile Builder – U Profile & User Registration Forms", which is version 3.6.5 at the time of this publication.

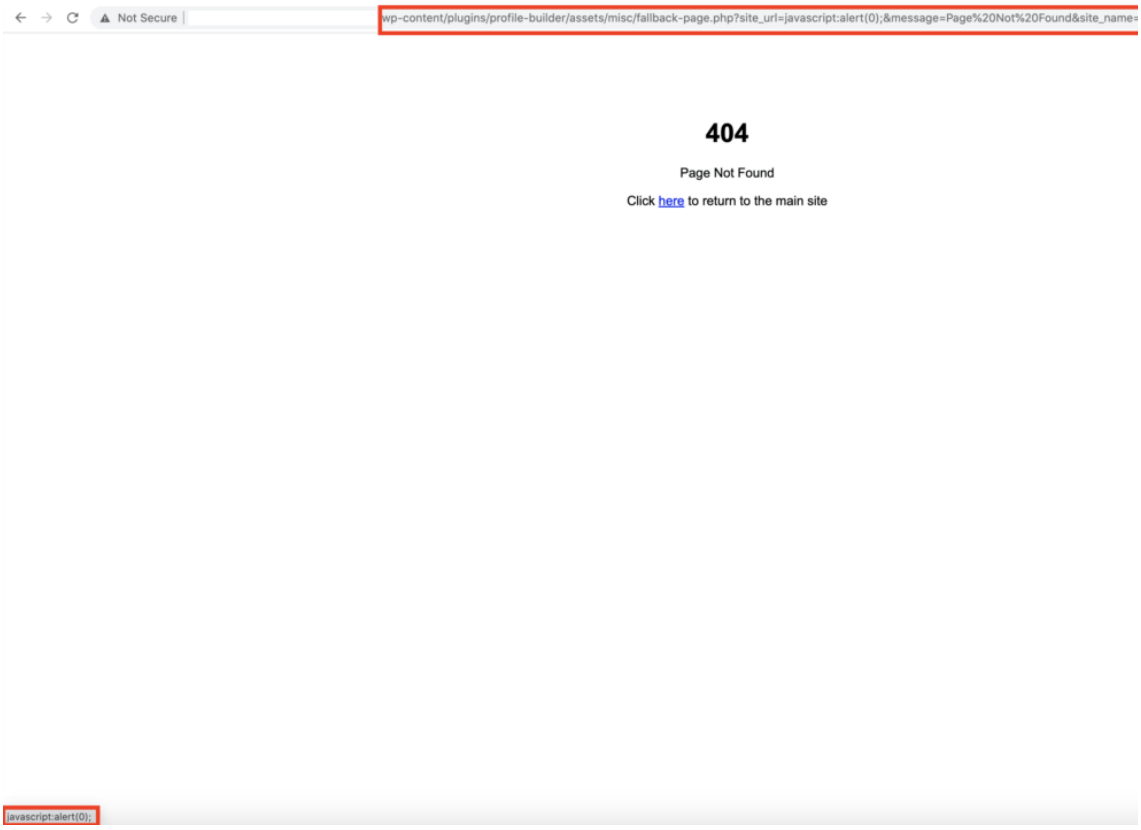
Description: Reflected Cross-Site Scripting
Affected Plugin: Profile Builder – User Profile & User Registration Forms
Plugin Slug: profile-builder
Plugin Developer: Cozmoslabs
Affected Versions: <= 3.6.1
CVE ID: CVE-2022-0653
CVSS Score: 6.1 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.6.2

Profile Builder – User Profile & User Registration Forms is a plugin designed to add enhanced user profile and registration capabilities to a WordPress site. The vulnerability in the plugin was simple

was no activation page selected for the user activation email functionality. Unfortunately, this file used the user supp value from the `site_url` parameter with insufficient sanitization/escaping and validation in an 'href' attribute which meant that it was possible for attackers to use the JavaScript pseudo protocol, `javascript:`, to inject malicious scri

```
<?php
define( 'ABSPATH', __DIR__ . '/' );//added this because we actually need to access this page directly, sorry about
/*
//load WP if needed
$path_to_wp_install_dir = '';
include_once ( $path_to_wp_install_dir.'wp-load.php' );
*/

if ( ! defined( 'ABSPATH' ) ) exit; // Exit if accessed directly

$site_name = ( isset( $_GET['site_name'] ) ? filter_var ( urldecode( $_GET['site_name'] ), FILTER_SANITIZE_STRING
$site_url = ( isset( $_GET['site_url'] ) ? filter_var ( urldecode( $_GET['site_url'] ), FILTER_SANITIZE_STRING ) :
$message = ( isset( $_GET['message'] ) ? filter_var ( urldecode( $_GET['message'] ), FILTER_SANITIZE_STRING ) : ''
?>

<html>
   <head>
      <style type="text/css">
         body {font-family:Arial; padding: 5px; margin-top:100px; text-align: center;}
      </style>

      <title><?php echo htmlspecialchars( $site_name, ENT_QUOTES ); // phpcs:ignore WordPress.Security.EscapeOutpu
   </head>

   <body id="wppb_content">
      <h1><?php echo htmlspecialchars( $site_name, ENT_QUOTES ); // phpcs:ignore WordPress.Security.EscapeOutput.O

      <?php echo '<p>'. htmlspecialchars( strip_tags( $message ) ). '</p>'; // phpcs:ignore WordPress.Security.Esc

      <?php echo 'Click <a href="'. htmlspecialchars(  $site_url, ENT_QUOTES ) .'">here</a> to return to the main
   </body>
</html></pre>
<pre>
```

Due to the fact that the attacker could also control some of the data on the page via the `site_name` and `message` parameter, an attacker could format it to look like it was a 404 page containing a link that the user needs to click in or to return to the site, which helps make it significantly less suspicious than other possible ways the payload could hav been presented. If a user clicked the link from "Click here" it would trigger the execution of the JavaScript.



Cross-Site Scripting vulnerabilities can be exploited to perform several actions like creating new administrative user accounts, injecting theme and plugin files with backdoors, and redirecting visitors to malicious sites, all of which can

reminder for site administrators and users to follow security best practices and avoid clicking on links from untrusted sources.

This vulnerability could also be used to redirect the user to a malicious site by simply injecting any domain in the `site_` parameter.

Timeline

January 4, 2022 – Conclusion of the plugin analysis that led to the discovery of a Reflected Cross-Site Scripting Vulnerability in the "Profile Builder – User Profile & User Registration Forms" plugin. We verify that the Wordfence firev provides sufficient coverage. We initiate contact with the developer.
January 5, 2022 – The developer confirms the inbox for handling the discussion.
January 6, 2022 – We send over the full disclosure details. The developer acknowledges the report and indicates tha they will work on a fix.
January 10, 2022 – A fully patched version of the plugin is released as version 3.6.2.

Conclusion

In today's post, we detailed a flaw in the "Profile Builder – User Profile & User Registration Forms" plugin that made it possible for unauthenticated attackers to inject malicious JavaScript onto a vulnerable site that would execute whenever an unsuspecting user clicked on a link containing the malicious payload. This flaw has been fully patched i version 3.6.2.

We recommend that WordPress site owners immediately verify that their site has been updated to the latest patchec version available, which is version 3.6.5 at the time of this publication.

All Wordfence users, including users of our Free, Premium, Care, and Response products are protected from exploits targeting this vulnerability thanks to the Wordfence Firewall's built-in Cross-Site Scripting (XSS) protection.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incid Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support i case you need further assistance.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory them to help keep their sites protected, as this is a serious vulnerability that can lead to complete site takeover.

Comments

No Comments

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

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.

Stay Updated

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

you@example.com

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

SIGN UP