Chloe Chamberland

June 28, 2021

Easily Exploitable Critical Vulnerabilities Patched in ProfilePress Plugin

On May 27, 2021, the Wordfence Threat Intelligence team initiated the responsible disclosure process for several vulnerabilities that were discovered in ProfilePress, formerly WP User Avatar, a WordPress plugin installed on over 400,000 sites. These flaws made it possible for an attacker to upload arbitrary files to a vulnerable site and register as an administrator on sites even if user registration was disabled, all without requiring any prior authentication.

We initially reached out to the plugin's developer on May 27, 2021. After receiving confirmation of an appropriate communication channel, we provided the full disclosure details the same day. An updated copy of the plugin was sent to our team on May 28, 2021, which we confirmed provided sufficient protection. The patch was quickly released on May 30, 2021 as version 3.1.4.

These are critical and easily exploitable security issues that have been patched, therefore, we highly recommend updating to the latest patched version available, 3.1.8, immediately if you are running a vulnerable version of this plugin (3.0- 3.1.3).

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on May 27, 2021. Sites still using the free version of Wordfence received the same protection on June 26, 2021.

We waited 30 days before disclosing these issues to ensure both Wordfence Premium and free users were protected against any exploit attempts given the severity of the issues and size of the installation base. We have also intentionally minimized the details provided on how these vulnerabilities could be exploited to delay any efforts by malicious threat actors.

Description: Unauthenticated Privilege Escalation
Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34621
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4

ProfilePress, formerly known as WP User Avatar, is a WordPress plugin that was originally designed to be used only to upload user profile photos. Recently, however, the plugin underwent a somewhat controversial revamp. The updated plugin introduced new features like user login and registration, while keeping the original profile photo uploading functionality, in order to create a robust user registration plugin. Unfortunately, the new features introduced several security issues.

The first issue discovered allowed users to escalate their privileges, which could lead to site takeover. During user registration, users could supply arbitrary user meta data that would get updated during the registration process. This included the `wp_capabilities` user meta that controls a user's capabilities and role. This made it possible for a user to supply `wp_capabilties` as an array parameter while registering, which would grant them the supplied capabilities, allowing them to set their role to any role they wanted, including administrator.

```
318  if (is_array($custom_usermeta)) {
319
320      foreach ($custom_usermeta as $key => $value) {
321          if ( ! empty($value)) {
322              update_user_meta($user_id, $key, $value);
323              // the 'edit_profile' parameter is used to distinguish it from same action hook in RegistrationAuth
324              do_action('ppress_after_custom_field_update', $key, $value, $user_id, 'registration');
325          }
326      }
327  }
```

In addition, there was no check to validate that user registration was enabled on the site, making it possible for users to register as an administrator even on sites where user registration was disabled. This meant that attackers could completely take over a vulnerable WordPress site without much effort if a vulnerable version of this plugin was in use.

Description: Authenticated Privilege Escalation
Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34622
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4

The same flaw was present within the user profile update functionality. The profile update functionality had the same feature that would take the key value pairs submitted during a profile update and update the user's metadata in the database. The `wp_capabilities` user meta could be supplied as an array parameter set to administrator during a profile update which would allow attackers to escalate their privileges to that of an administrator.

```
if (is_array($custom_usermeta)) {
```

```
            update_user_meta($user_id, $key, $value);

            // the 'edit_profile' parameter is used to distinguish it from same action hook in RegistrationAuth
            do_action('ppress_after_custom_field_update', $key, $value, $user_id, 'edit_profile');
        }
    }
```

This did require the attacker to have an account on a vulnerable site to exploit. However, since the registration function did not validate if user registration was enabled, a user could easily sign up and exploit this vulnerability, if they were not able to exploit the privilege escalation vulnerability during registration.

Description: Arbitrary File Upload in Image Uploader Component
Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0 – 3.1.3
CVE ID: CVE-2021-34623
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4

In addition to the privilege escalation vulnerabilities, we found that arbitrary files, including PHP files, could be uploaded to a vulnerable WordPress site. The ability to upload profile and cover images to a user's profile is a core part of the plugin's functionality. Unfortunately, this function was insecurely implemented using the `exif_imagetype` function to determine a file's type.

```
// verify the file is a GIF, JPEG, or PNG
$fileType = exif_imagetype($image["tmp_name"]);

$allowed_image_type = apply_filters('ppress_allowed_image_type', array(
    IMAGETYPE_GIF,
    IMAGETYPE_JPEG,
    IMAGETYPE_PNG
));
```

The function `exif_imagetype` uses the first few bytes of a file, known as magic bytes, to determine a file's type, and as such is considered an unsafe method to validate a file's type. Any file can trivially be disguised to appear as a valid image file by adding these magic bytes to the beginning of the file. This made it possible for an attacker to upload a spoofed PHP file that would pass the `exif_imagetype` check during the user registration process or during a profile update.

This could be used to upload a webshell that would make it possible for an attacker to achieve remote code execution and run commands on a server to achieve complete site takeover. Due to the fact that users could register even without user registration enabled, any attacker could exploit this vulnerability without authentication by uploading a profile picture or cover image during a registration request.

Description: Arbitrary File Upload in File Uploader Component
Affected Plugin: User Registration, User Profiles, Login & Membership – ProfilePress (Formerly WP User Avatar)
Plugin Slug: wp-user-avatar
Affected Versions: 3.0- 3.1.3
CVE ID: CVE-2021-34624
CVSS Score: 9.8 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 3.1.4

In addition to the previous arbitrary file upload vulnerability, we discovered that another endpoint was also vulnerable to arbitrary file uploads. It appears that there was functionality in the plugin to upload files to a user's profile account during user registration or during a profile update if a site was using the plugin's "custom fields" extension.

This function performed a file extension check only if a set of extensions was supplied by a site administrator via a custom field on the registration and profile update page. This meant that if a site administrator didn't configure file uploads for the user registration and profile page using custom fields, then any file type would be allowed due to the extensions field being empty.

This made it possible for attackers to upload arbitrary files to a site during the user registration process or during a profile update, as long as an administrator didn't configure the file upload settings. Again, this could be used to upload a webshell and obtain remote code execution to take over a site.

Disclosure Timeline

May 27, 2021 – Conclusion of the plugin analysis that led to the discovery of several vulnerabilities in the ProfilePress plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users.
May 27, 2021 6:27 PM UTC – We initiate contact with the plugin developer.
May 27, 2021 6:52 PM UTC – The plugin developer confirms the inbox for handling discussion.
May 27, 2021 9:23 PM UTC – We send over full disclosure details.
May 27, 2021 9:27 PM UTC – The plugin developer confirms they have received the details and will begin working on a fix.
May 28, 2021 7:16 AM UTC – The plugin developer sends us a copy of the proposed patches.
May 28, 2021 12:48 PM UTC – We inform the developer that we will review the patches and get back to them as soon as our analysis is complete.
May 28, 2021 3:44 PM UTC – We confirm the patches are sufficient and inform the developer.
May 30, 2021 – A newly updated version of the plugin containing the patches is released.
June 26, 2021 – Free Wordfence users receive firewall rules.

Conclusion

In today's post, we detailed several critical flaws in ProfilePress that granted attackers the ability to upload malicious files to achieve remote code execution in addition to registering as an administrator. These flaws have been fully patched in version 3.1.4. We recommend that users immediately update to the latest version available, which is version 3.1.8 at the time of this publication, if they are running a vulnerable version of the plugin (3.0 – 3.1.3).

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on May 27, 2021. Sites still using the free version of Wordfence received the same protection on June 26, 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 critical severity vulnerabilities that can be easily exploited.

Special thanks to Collins at ProfilePress for working quickly to get a sufficient patch out to protect users.
Did you enjoy this post? Share it!

Comments

9 Comments

Jos Klever *
June 28, 2021
2:00 pm

I'm glad I've removed the plugin from sites that used it, as soon as WP User Avatar was replaced by the totally different plugin ProfilePress. That should have been forbidden, because this wasn't an update, but a replacement and should have been thoroughly

Thanks for making it safer for the remaining users.

Patrick Waara *
June 28, 2021
2:04 pm

To be clear, these vulnerabilities did not exist in the previous versions (2.2.16 and below), correct?

Chloe Chamberland *
June 29, 2021
6:43 am

Hi Patrick,

That is correct! These vulnerabilities only affected versions 3.0 - 3.1.3. If you are running anything under version 3.0 or above version 3.1.3 then your site is not affected by these vulnerabilities.

Mark *
June 28, 2021
3:25 pm

I had installed this plugin initially on two client sites when it was still "WP User Avatar". When it turned into a membership plugin of sorts, I removed it because the clients were still on a maintenance plan with me. And this was not what we had wanted.

While I appreciate code vulernabilities and oversights can happen, I wish they didn't switch the core premise of the plugin from the original custom image one to a community and membership style plugin. I would not then have been watching my back for this type of "registration" vulnerability.

Gareth Griffiths *
June 29, 2021
2:31 am

Great work, guys.

Am I right in thinking that a site that does not use the standard "wp_" table prefix is protected against the capabilities injection?

Ram Gall *
July 15, 2021
2:36 pm

Hi Gareth,

Unfortunately the wp_ prefix in wp_capabilities is not related to the database table prefix so changing the table prefix would not protect against this vulnerability.

RB *
July 1, 2021
6:45 pm

I thought I had deleted all incarnations of ProfilePress on the websites I manage, but one still existed. This eve, I got a notification that a new user registered, using two different user names. I deleted ProfilePress, changed the website's passwords and added the user's IP to Wordfence's block IP list. Is this enough? What more should I do?

Chloe Chamberland *
July 12, 2021
10:32 am

Hi Renee,

I am sorry to hear that one of your sites was affected by these vulnerabilities! You have performed the right first steps. I recommend following this guide to ensure your site has no remnants of malware after those two administrative user accounts have been removed. If you have any questions please don't hesitate to reach out to our support team!

KP *
July 11, 2021
8:19 pm

Wow, this is very alarming. I used to use WP User Avatar but stopped once ProfilePress took over. These type of take overs should not be allowed in the WP Repo. Very dangerous!

SIGN UP