WordPress Advanced Custom Fields Extended Plugin Vulnerability via @sejournal, @martinibuster



An advisory was published about a vulnerability in the popular Advanced Custom Fields: Extended WordPress plugin that is rated 9.8, affecting up to 100,000 installations.

The flaw enables unauthenticated attackers to register themselves with administrator privileges and gain full control of a website and all settings.

Advanced Custom Fields: Extended Plugin

The Advanced Custom Fields: Extended plugin is an add-on to the popular Advanced Custom Fields Pro plugin. It is used by WordPress site owners and developers to extend how custom fields work, manage front-end forms, create options pages,

define custom post types and taxonomies, and customize the WordPress admin experience.

The plugin is widely used, with more than 100,000 active installations, and is commonly deployed on sites that rely on front-end forms and advanced content management workflows.

Who Can Exploit This Vulnerability

This vulnerability can be exploited by unauthenticated attackers, which means there is no barrier of first having to attain a higher permission level before launching an attack. If the affected version of the plugin is present with a specific configuration in place, anyone on the internet can attempt to exploit the flaw. That kind of exposure significantly increases risk because it removes the need for compromised credentials or insider access.

Privilege Escalation Exposure

The vulnerability is a privilege escalation flaw caused by missing role restrictions during user registration.

Specifically, the plugin’s insert_user function does not limit which user roles can be assigned when a new user account is created by anyone. Under normal circumstances, WordPress should strictly control which roles users can select or be assigned during registration.

Because this check is missing, an attacker can submit a registration request that explicitly assigns the administrator role to the new account.

This issue only occurs when the site’s form configuration maps a custom field directly to the WordPress role field. When that condition is met, the plugin accepts the supplied role value without verifying that it is safe or permitted.

The flaw appears to be due to insufficient server-side validation of the form field “Choices.” The plugin seems to have relied on the the HTML form to restrict which roles a user could select. For example, the developer could create a user sign up form with only the “subscriber” role as an option. But there was no verification on the backend to check if the user role the subscriber was signing up with matched the user roles that the form is supposed to be limited to.

What was probably happening is that an unauthenticated attacker could inspect the form’s HTML, see the field responsible for the user role, and intercept the HTTP request so that, for example, instead of sending role=subscriber, the attacker could change the value to role=administrator. The code responsible for the insert_user action took this input and passed it directly to WordPress user creation functions. It did not check if “administrator” was actually one of the allowed options in the field’s “Choices” list.

The Changelog for the plugin lists the following entry as one of the patches to the plugin:

> *“Enforced front-end fields validation against their respective “Choices” settings.”*

That entry in the changelog means the plugin now actively checks front-end form submissions to ensure the submitted value matches the field’s defined “Choices”, rather than trusting whatever value is posted.

There is also this entry in the changelog:

> *“Module: Forms – Added security measure for forms allowing user role selection”*

This entry means the plugin added server-side protections to prevent abuse when a front-end form is allowed to set or select a WordPress user role.

Overall, the patches to the plugin added stronger validation controls for front-end forms plus made them more configurable.

What Attackers Can Gain

If successfully exploited, the attacker gains administrator-level access to the WordPress site.

That level of access allows attackers to:

- Install or modify plugins and themes
- Inject malicious code
- Create backdoor administrator accounts
- Steal or manipulate site data
- Redirect visitors or distribute malware

Gaining administrator access is a full site takeover.

The Wordfence advisory describes the issue as follows:

> *“The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 0.9.2.1. This is due to the ‘insert_user’ function not restricting the roles with which a user can register. This makes it possible for unauthenticated attackers to supply the ‘administrator’ role during registration and gain administrator access to the site.”*

As Wordfence describes, the plugin trusts user-supplied input for account roles when it should not. That trust allows attackers to bypass WordPress’s normal protections and grant themselves the highest possible permission level.

Wordfence also reports having blocked active exploitation attempts targeting this vulnerability, indicating that attackers are already probing sites for exposure.

Conditions Required For Exploitation

The vulnerability is not automatically exploitable on every site running the plugin.

Exploitation requires that:

- The site uses a front-end form provided by the plugin
- The form maps a custom field directly to the WordPress user role

Patch Status and What Site Owners Should Do

The vulnerability affects all versions up to and including 0.9.2.1. The issue is addressed in version 0.9.2.2, which introduces additional validation and security checks around front-end forms and user role handling.

The entry for the official changelog for ACF Extended Basic 0.9.2.2:

- *Module: Forms – Enforced front-end fields validation against their respective "Choices" settings*
- *Module: Forms – Added security measure for forms allowing user role selection*
- *Module: Forms – Added acfe/form/validate_value hook to validate fields individually on front*
- *Module: Forms – Added acfe/form/pre_validate_value hook to bypass enforced validation*

Site owners using this plugin should update immediately to the latest patched version. If updating is not possible, the plugin should be disabled until the fix can be applied.

Given the severity of the flaw and the lack of authentication required to exploit it, delaying action leaves affected sites exposed to a complete takeover.

Featured Image by Shutterstock/Art Furnace

https://www.searchenginejournal.com/wordpress-acf-extended-plugin-vulnerability/565483/