10 years CERT-EU

Security Advisory 2023-027

Critical Vulnerability in Wordpress Plugins

May 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/05/2023 — v1.0 – Initial publication*

Summary

A reflected XSS vulnerability has been discovered in the Advanced Custom Fields (ACF) and Advanced Custom Fields Pro WordPress plugins (versions 6.1.5 and below). This vulnerability allows unauthenticated users to potentially escalate privileges on a WordPress site by tricking a privileged user into visiting a maliciously crafted URL. The issue has been fixed in version 6.1.6, and has been assigned CVE-2023-30777 [1, 2].

Technical Details

The vulnerability is found within the `admin_body_class` function in the file:

`includes/admin/admin-internal-post-type-list.php`

This function is an extra handler for the `admin_body_class` WordPress hook, which is responsible for filtering CSS classes for the main body tag in the admin area. The outputted value of the hook is not properly sanitised and is directly constructed on the HTML page.

The `admin_body_class` function concatenates the `$this->view` variable to the `$classes` variable, which is then returned as the classes string. However, the sanitisation using the `sanitize_text_field` function is insufficient to prevent XSS, as it allows for a DOM XSS payload.

Affected Products

The affected products are:

- Advanced Custom Fields WordPress plugin (Free version), versions 6.1.5 and below.
- Advanced Custom Fields Pro WordPress plugin (Pro version), versions 6.1.5 and below.

Recommendations

To mitigate this vulnerability, users should update the respective plugins to at least version 6.1.6.

References

[1] https://patchstack.com/articles/reflected-xss-in-advanced-custom-fields-plugins-affecting-2-million-sites/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30777