بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

آسیب پذیری افزونه‌های وردپرس

گزارش آسیب پذیری

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۴۰۲/۰۲/۱۷

طبقه‌بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۴۲۶۵۰۰۰۰

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ مقدمه

محققان امنیتی Patchstack اخیراً هشدار داده‌اند که افزونه‌های وردپرس « Advanced Custom Fields» و «Advanced Custom Fields Pro» در معرض خطر حملات XSS قرار دارند.

این افزونه‌های وردپرسی که در میلیون‌ها وب‌سایت نصب شده‌اند، ممکن است در برابر نقض‌های امنیتی آسیب‌پذیر باشند.

افزونه‌های«Advanced Custom Fields» و «Advanced Custom Fields Pro» بیلدرهای فیلد سفارشی معروف در وردپرس هستند و با بیش از ۲ میلیون نصب فعال، پایگاه کاربری قابل توجهی را جمع‌آوری کرده‌اند.

آسیب‌پذیری XSS توسط محقق Patchstack در ۲ مه ۲۰۲۳، شناسایی و با عنوان «CVE-2023-30777» پیگیری شده‌است.

۲ جزئیات فنی آسیب‌پذیری

۲-۱ آسیب‌پذیری در Advanced Custom Fields

آسیب‌پذیری‌های XSS دروازه‌ای را برای عاملان تهدید فراهم می‌کند تا اسکریپت‌های مضر را به وب‌سایت‌های در دسترس کاربران ناآگاه تزریق کنند. این کد در مرورگر بازدیدکننده اجرا می‌شود و امنیت کاربران را به خطر می‌اندازد. بر اساس Patchstack، مهاجم می‌تواند از آسیب‌پذیری XSS برای سرقت داده‌های محرمانه استفاده کند و حتی دسترسی خود را در سایت وردپرس تحت حمله بالا ببرد.

توجه به این نکته ضروری است که این نقص خاص همچنین می‌تواند در نصب یا پیکربندی پیش‌فرض افزونه Advanced Custom Fields نیز فعال شود.

برای بهره‌برداری از این آسیب‌پذیری، عامل تهدید می‌بایست تاکتیک‌های مهندسی اجتماعی را نیز بکار برد تا فردی را که به افزونه دسترسی دارد، متقاعد کند که از یک URL مخرب بازدید کند. به طور خلاصه، این آسیب‌پذیری نمی‌تواند از طریق حمله مستقیم توسط مهاجم ایجاد شود.

به محض این‌که Patchstack آسیب‌پذیری را به اطلاع توسعه دهنده پلاگین قرار داد، اقدامی فوری اتخاذ شد و آن‌ها به سرعت یک به‌روزرسانی امنیتی را در ۴ می ۲۰۲۳ منتشر کردند که این مشکل را برطرف نمود و اکنون به عنوان نسخه ۶,۱,۶ در دسترس است.

این آسیب‌پذیری (CVE-2023-30777) ناشی از handler تابع «admin_body_class» است. ضمن اینکه این handler به اندازه کافی مقدار خروجی مدیریت کننده کلاس‌های CSS را پاکسازی نکرد.

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

```
public function admin_body_class( $classes ) {
    $classes .= " acf-admin-page acf-internal-post-type {$this->admin_body_class}";

    if ( $this->view ) {
        $classes .= " view-{$this->view}";
    }

    return $classes;
}
```

شکل۱. تابع admin_body_class

در کد افزونه، مهاجم می‌تواند از یک متغیر توالی کد مستقیم ناامن ('$this→view')، استفاده نماید. مهاجمان با بهره‌برداری از این تهدید، کدهای مخربی مانند کدهای DOM XSS را به بخش‌هایی که در نهایت به یک رشته کلاس منتقل می‌شوند، اضافه نمایند.

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

```
public function current_screen() {
    // Bail early if not the list admin page.
    if ( ! acf_is_screen( "edit-{$this->post_type}" ) ) {
        return;
    }

    // Get the current view.
    $this->view = isset( $_GET['post_status'] ) ? sanitize_text_field( $_GET['post_sta
-----------------------------------
```

شکل۲. افزودن کد مخرب

علاوه بر این، شایان ذکر است که تابع پاکسازی پلاگین «sanitize_text_field» قادر به جلوگیری از این حمله نخواهد بود به این خاطر که پلاگین مذکور، نمی‌تواند کد مخرب تزریق شده را شناسایی و خنثی کند. بنابراین، کد تزریق شده همچنان می‌تواند از تابع عبور کند و به طور بالقوه باعث آسیب شود.

در نسخه 6.1.6 این افزونه، توسعه دهنده با معرفی یک تابع جدید به نام «esc_attr» این آسیب‌پذیری را رفع نمود.

این تابع پاکسازی کاملی را روی مقدار خروجی تابع «admin_body_class» انجام می‌دهد و به طور موثر از وقوع هرگونه حمله XSS جلوگیری می‌نماید.

۲-۲ زمانبندی افشا

در زیر، زمانبندی افشا ذکر شده است:

۲۰۲۳-۰۵-۰۲: کارشناسان، آسیب‌پذیری را پیدا کردند و با فروشنده افزونه تماس برقرار کردند.

۲۰۲۳-۰۵-۰۴: نسخه 6.1.6 افزونه‌های «Advanced Custom Fields» و « Advanced Custom Fields Pro » برای اصلاح مشکلات گزارش شده منتشر شد.

۲۰۲۳-۰۵-۰۵: آسیب‌پذیری‌ها به پایگاه داده آسیب‌پذیری Patchstack اضافه شد.

۳ توصیه‌های امنیتی

تحلیلگران امنیت سایبری اکیداً توصیه کرده‌اند که همه کاربران « Advanced Custom Fields» و «Advanced Custom Fields Pro» فوراً به نسخه ۶,۱,۶ یا نسخه جدیدتر ارتقا یابند.

انجام این کار آسیب‌پذیری را وصله می نماید و از وب سایت‌ها در برابر نقض احتمالی امنیتی محافظت می‌کند.

۴ منابع

[1] https://cybersecuritynews.com/over-2-million-wordpress-websites-exposed-to-xss-attacks/