بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش آسیب‌پذیری Wordpress_Essential Addons for Elementor

گزارش فنی

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۴۰۲/۰۲/۲۴

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر - پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ شرح آسیب‌پذیری

محققین Patchstack یک آسیب پذیری با شناسه CVE-2023-32243 و دارای شدت بحرانی در پلاگین وردپرس به نام Essential Addons for Elementor معرفی کردند. آسیب پذیری CVE-2023-32243 در این پلاگین، امکان افزایش امتیاز را به یک مهاجم بدون احرازهویت شده می‌دهد. مهاجم می‌تواند با ریست کردن پسورد هر کاربر، وارد اکانت آن شود. نکته دیگر آن است که مهاجم باید نام کاربری قربانی رو بداند و هچنین مهاجم می‌تواند اکانت مدیر سایت را با این آسیب پذیری بدست آورد و کل سایت را در دست بگیرد. علت کلی آسیب پذیری بدین شرح است که تابع ریست پسورد، بدون اینکه کلید ریست پسورد را بررسی و تایید کند، پسورد را مستقیما عوض میکند.

جدول نسخه های تحت تاثیر و اصلاح شده:

نسخه های اصلاح شده	نسخه های تحت تاثیر
نسخه ۵,۷,۲ به بالاتر	نسخه های ۵,۴,۰ تا ۵,۷,۱

کشف آسیب‌پذیری در این پلاگین با مشاهده init hook در تابع register_hooks آغاز شده است که در شکل زیر نشان داده شده است.

includes/Classes/Bootstrap.php

```
// Login | Register
add_action('init', [$this, 'login_or_register_user']);
```

در کد بالا ، تابع login_or_register_user اجرا می‌شود، این تابع بصورت زیر است:

includes/Traits/Login_Registration.php

```
public function login_or_register_user() {
    do_action( 'eael/login-register/before-processing-login-register', $_POST );
    // login or register form?
    if ( isset( $_POST['eael-login-submit'] ) ) {
        $this->log_user_in();
    } else if ( isset( $_POST['eael-register-submit'] ) ) {
        $this->register_user();
    } else if ( isset( $_POST['eael-lostpassword-submit'] ) ) {
        $this->send_password_reset();
    } else if ( isset( $_POST['eael-resetpassword-submit'] ) ) {
        $this->reset_password();
    }
    do_action( 'eael/login-register/after-processing-login-register', $_POST );

}
```

این تابع با بررسی برخی پارامترهای $_POST و فراخوانی توابع مربوطه، اقدام به بررسی صحت اطلاعات و ورود کاربر می‌کند. آسیب پذیری مربوط به تابع reset_password است. این تابع تنها در نسخه ۵,۴,۰ و بعد از آن وجود دارد.

includes/Traits/Login_Registration.php

```
public function reset_password() {
    $ajax    = wp_doing_ajax();
    $page_id = 0;
    if ( ! empty( $_POST['page_id'] ) ) {
        $page_id = intval( $_POST['page_id'], 10 );
    } else {
        $err_msg = esc_html__( 'Page ID is missing', 'essential-addons-for-elementor-lite' );
    }

    $widget_id = 0;
    if ( ! empty( $_POST['widget_id'] ) ) {
        $widget_id = sanitize_text_field( $_POST['widget_id'] );
    } else {
        $err_msg = esc_html__( 'Widget ID is missing', 'essential-addons-for-elementor-lite' );
    }

    $rp_data = [
        'rp_key' => ! empty( $_POST['rp_key'] ) ? sanitize_text_field( $_POST['rp_key'] ) : '',
        'rp_login' => ! empty( $_POST['rp_login'] ) ? sanitize_text_field( $_POST['rp_login'] ) :
'',
    ];

    update_option( 'eael_resetpassword_rp_data_' . esc_attr( $widget_id ), maybe_serialize(
$rp_data ), false );

    update_option( 'eael_show_reset_password_on_form_submit_' . $widget_id, true, false );

    if (!empty( $err_msg )){
        if ( $ajax ) {
            wp_send_json_error( $err_msg );
        }
        update_option( 'eael_resetpassword_error_' . $widget_id, $err_msg, false );

        if (isset($_SERVER['HTTP_REFERER'])) {
            wp_safe_redirect($_SERVER['HTTP_REFERER']);
            exit();
        }
    }
```

```
    if ( empty( $_POST['eael-resetpassword-nonce'] ) ) {
        $err_msg = esc_html__( 'Insecure form submitted without security token', 'essential-addons-for-elementor-lite' );
        if ( $ajax ) {
            wp_send_json_error( $err_msg );
        }
        update_option( 'eael_resetpassword_error_' . $widget_id, $err_msg, false );

        if (isset($_SERVER['HTTP_REFERER'])) {
            wp_safe_redirect($_SERVER['HTTP_REFERER']);
            exit();
        }
    }
    if ( ! wp_verify_nonce( $_POST['eael-resetpassword-nonce'], 'essential-addons-elementor' ) ) {
        $err_msg = esc_html__( 'Security token did not match', 'essential-addons-for-elementor-lite' );
        if ( $ajax ) {
            wp_send_json_error( $err_msg );
        }
        update_option( 'eael_resetpassword_error_' . $widget_id, $err_msg, false );

        if (isset($_SERVER['HTTP_REFERER'])) {
            wp_safe_redirect($_SERVER['HTTP_REFERER']);
            exit();
        }
    }
    $settings = $this->lr_get_widget_settings( $page_id, $widget_id);

    if ( is_user_logged_in() ) {
        $err_msg = isset( $settings['err_loggedin'] ) ? __( Helper::eael_wp_kses( $settings['err_loggedin'] ), 'essential-addons-for-elementor-lite' ) : esc_html__( 'You are already logged in', 'essential-addons-for-elementor-lite' );
        if ( $ajax ) {
            wp_send_json_error( $err_msg );
        }
        update_option( 'eael_resetpassword_error_' . $widget_id, $err_msg, false );

        if (isset($_SERVER['HTTP_REFERER'])) {
            wp_safe_redirect($_SERVER['HTTP_REFERER']);
            exit();
        }
    }

    do_action( 'eael/login-register/before-resetpassword-email' );
```

```
    $widget_id = ! empty( $_POST['widget_id'] ) ? sanitize_text_field( $_POST['widget_id'] ) : '';


    // Check if password is one or all empty spaces.
    $errors = [];
    if ( ! empty( $_POST['eael-pass1'] ) ) {
        $post_eael_pass1 = trim( $_POST['eael-pass1'] );


        if ( empty( $post_eael_pass1 ) ) {
            $errors['password_reset_empty_space'] = isset( $settings['err_pass'] ) ? __(
Helper::eael_wp_kses( $settings['err_pass'] ), 'essential-addons-for-elementor-lite' ) :
esc_html__( 'The password cannot be a space or all spaces.', 'essential-addons-for-elementor-lite'
);
        }
    } else {
        if ( empty( $_POST['eael-pass1'] ) ) {
            $errors['password_reset_empty_space'] = isset( $settings['err_pass'] ) ? __(
Helper::eael_wp_kses( $settings['err_pass'] ), 'essential-addons-for-elementor-lite' ) :
esc_html__( 'The password cannot be a space or all spaces.', 'essential-addons-for-elementor-lite'
);
        }
    }


    if( ! empty( $_POST['eael-pass1'] ) && strlen( trim( $_POST['eael-pass1'] ) ) == 0 ){
        $errors['password_reset_empty'] = esc_html__( 'The password cannot be empty.', 'essential-
addons-for-elementor-lite' );
    }


    // Check if password fields do not match.
    if ( ! empty( $_POST['eael-pass1'] ) && $_POST['eael-pass2'] !== $_POST['eael-pass1'] ) {
        $errors['password_reset_mismatch'] = isset( $settings['err_conf_pass'] ) ? __(
Helper::eael_wp_kses( $settings['err_conf_pass'] ), 'essential-addons-for-elementor-lite' ) :
esc_html__( 'The passwords do not match.', 'essential-addons-for-elementor-lite' );
    }


    if ( ( ! count( $errors ) ) && isset( $_POST['eael-pass1'] ) && ! empty( $_POST['eael-pass1'] )
) {
        $rp_login = isset( $_POST['rp_login']) ? sanitize_text_field( $_POST['rp_login'] ) : '';
        $user = get_user_by( 'login', $rp_login );


        if( $user || ! is_wp_error( $user ) ){
            reset_password( $user, sanitize_text_field( $_POST['eael-pass1'] ) );
--------------------------------------------------------------------------------
```

برای شروع، مقدار تصادفی در $_POST['page_id'] و $_POST['widget_id'] تنظیم می‌کنیم تا برای دور زدن این دو مورد متغیر $err_msg تنظیم نشود.

همچنین در ادامه باید $_POST['eael-resetpassword-nonce'] را نیز تنظیم کنیم زیرا مقدار nonce بر روی کد بررسی خواهد شد. برای تنظیم رمزعبور، باید همان رشته رمزعبور را در $_POST['eael-pass1'] و $_POST['eael-pass2'] تأمین کنیم چرا که بررسی خواهد شد.

اگر همه مراحل بالا رو پشت سر گذاشته شود، متغیر $rp_login از $_POST[‘rp_login'] مقدار دهی می‌شوند.

در ادامه کد ، با استفاده از تابع get_user_by دنبال مقدار login (username) که با مقدار $rp_login مطابقت دارد را پیدا می‌کند و در متغیر $user قرار می‌دهد. حالا اگر $user وجود داشته باشد و خطایی نیز رخ ندهد، رمز با استفاده از تابع reset_password ، مستقیما ریست می‌شود.

تقریبا همه مراحل بالا به جز بدست آوردن مقدار essential-addons-elementor nonce قابل دور زدن است. این مقدار در صفحه اصلی وردپرس است، چون متغیر $this->localize_objects توسط تابع load_commnon_asset تنظیم می‌شود.

includes/Classes/Asset_Builder.php

```php
// localize object
$this->localize_objects = apply_filters( 'eael/localize_objects', [
    'ajaxurl'            => admin_url( 'admin-ajax.php' ),
    'nonce'              => wp_create_nonce( 'essential-addons-elementor' ),
```

متغیر $this->localize_objects که در کد بالا مقدار دهی شد، در تابع frontend_asset_load به عنوان شی برای تابع wp_localize_script استفاده خواهد شد.

includes/Classes/Asset_Builder.php

```php
public function frontend_asset_load() {
    $handle        = 'eael';
    $this->post_id = get_the_ID();

    $this->elements_manager->get_element_list( $this->post_id );
    $this->load_commnon_asset();
    $this->register_script();

-------------------- CUTTED HERE ------------------------------------

    wp_localize_script( $handle, 'localize', $this->localize_objects );
}
```

تابع frontend_asset_load هم از طریق تابع init_hook فراخوانی می‌شود و همانطور که در کد بالا مشاهده می‌کنید به عنوان یک تابع کنترل کننده (function handler) ،هوک wp_enqueue_scripts مورد استفاده قرار می‌گیرد. wp_enqueue_scripts برای نمایش همه اسکریپت‌ها و استایل‌های صف بندی شده مورد استفاده قرار میگیرند.

اصلاح:

توسعه دهنده برای اصلاح این آسیب پذیری از مقدار eael_resetpassword_rp_data که توسط تابع eael_redirect_to_reset_password مقداردهی می‌شود، استفاده کرده است.

۲ مراجع

https://patchstack.com/articles/critical-privilege-escalation-in-essential-addons-for-elementor-plugin-affecting-1-million-sites/