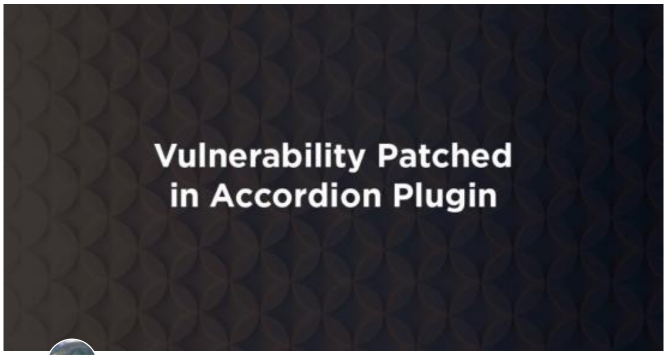


Chloe Chamberland

April 14, 2020

Vulnerability Patched in Accordion Plugin

A few weeks ago, our Threat Intelligence team discovered a vulnerability in Accordion, a WordPress plugin installed on over 30,000 sites. This flaw allowed any authenticated user with subscriber-level and above permissions the ability to import a new accordion and inject malicious Javascript as part of the accordion.

We initially reached out to the plugin's developer on March 10, 2020, however, an appropriate communication channel was not established until March 18, 2020. A patch was released just 3 hours after full disclosure.

This is considered a medium-level security issue that could potentially lead to attackers completely taking over WordPress sites. We highly recommend an immediate update to the latest version available, 2.2.15.

Wordfence Premium customers received a new firewall rule on March 10, 2020, to protect against exploits targeting this vulnerability. Free Wordfence users received this rule after thirty days, on April 9, 2020.

Description: Unprotected AJAX Action to Stored/Reflected Cross-Site Scripting (XSS)
Affected Plugin: Accordion
Plugin Slug: accordions
Affected Versions: <= 2.2.8
CVE ID: CVE-2020-13644
CVSS Score: 5.4 (Medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
Fully Patched Version: 2.2.9

The Accordion plugin is a relatively simple plugin used to create accordion style FAQ pages and knowledge base areas on WordPress sites. As part of the plugin's functionality, users can import new accordions, so that accordions can be exported on one site and migrated to another or even used to restore accordion backups.

In order to provide this functionality, the plugin registers an AJAX action that is used to register the import of a JSON file and its contents as a new accordion.

```php
add_action('wp_ajax_accordions_ajax_import_json', 'accordions_ajax_import_json');
//add_action('wp_ajax_nopriv_accordions_ajax_import_json', 'accordions_ajax_import_json');
```

This action is hooked to the function `accordions_ajax_import_json` where the data from the JSON file is extracted, analyzed, and used to create a new post with the post_type set to 'accordions.'

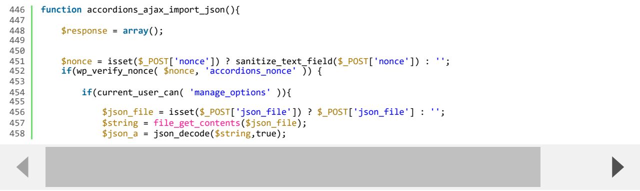
```php
function accordions_ajax_import_json(){

    $response = array();
    $json_file = isset($_POST['json_file']) ? $_POST['json_file'] : '';
    $string = file_get_contents($json_file);
    $json_a = json_decode($string,true);


    foreach ($json_a as $post_id=>$post_data){

        $meta_fields = $post_data['meta_fields'];
        $title = $post_data['title'];

        // Create post object
        $my_post = array(
            'post_title'    => $title,
            'post_type' => 'accordions',
            'post_status'   => 'publish',

        );

        $post_inserted_id = wp_insert_post( $my_post );

        foreach ($meta_fields as $meta_key=>$meta_value){
            update_post_meta( $post_inserted_id, $meta_key, $meta_value );
        }




    }


    $response['json_a'] = $json_a;
    //$response['string'] = $string;
    //$response['json_file'] = $json_file;




    echo json_encode( $response );




    die();
}
```

Due to the lack of capability checks and the inherent ability of any user logged in to a WordPress site to execute AJAX actions, this meant that any authenticated user, including those with minimal permissions, could import a new accordion from a remotely hosted JSON file. Additionally, malicious Javascript could be included in the imported accordion, allowing an attacker to inject malicious code that would execute if an administrator accessed the imported accordion from the WordPress administrative dashboard. This is considered to be a Stored Cross-Site Scripting vulnerability.

Alternatively, an attacker could exploit this weakness by tricking a site owner into clicking on a link designed to import a specially crafted JSON file containing malicious Javascript.
As shown in the `accordions_ajax_import_json` function, the JSON file's contents are decoded at the start of the import and later echoed at the end of a successful import causing any malicious Javascript that was contained in the file to be executed in the victim's browser. This is considered to be a Reflected Cross-Site Scripting vulnerability.

If an attacker was able to successfully trick an administrator into accessing their maliciously uploaded accordion or clicking on a specially crafted link, they could obtain an administrative user account, redirect the site owner to a malicious site, or steal session cookies to authenticate onto the site on behalf of the administrator. This meant an attacker could completely take over a vulnerable site by exploiting these XSS flaws.

Fortunately, in the most up-to-date versions of this plugin, there is a nonce and capability check present for the `accordions_ajax_import_json` function as shown below:



```
function accordions_ajax_import_json(){

    $response = array();


    $nonce = isset($_POST['nonce']) ? sanitize_text_field($_POST['nonce']) : '';
    if(wp_verify_nonce( $nonce, 'accordions_nonce' )) {

        if(current_user_can( 'manage_options' )){

            $json_file = isset($_POST['json_file']) ? $_POST['json_file'] : '';
            $string = file_get_contents($json_file);
            $json_a = json_decode($string,true);
```

Disclosure Timeline

March 10, 2020 – Initial discovery and analysis of vulnerability. Firewall rule was released for Wordfence Premium customers. We made our initial contact attempt with the plugin development team.
March 18, 2020 – An appropriate communication channel was established and full disclosure details were sent. Patch was released just 3 hours after disclosure.
April 9, 2020 – Free Wordfence users received firewall rule.

Conclusion

In today's post, we detailed a flaw related to an unprotected AJAX action that allowed for malicious accordions to be imported in Accordion, a WordPress plugin. This flaw has been fully patched in version 2.2.9. We recommend that users immediately update to the latest version available. Sites running Wordfence Premium have been protected from attacks against this vulnerability since March 10, 2020. Sites running the free version of Wordfence received this firewall rule update on April 9, 2020.

Did you enjoy this post? Share it!

Comments

1 Comment

Link Store *
April 14, 2020
8:18 pm

Thanks for the timely information, I always believe Wordfence.

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service Privacy Policy

CCPA Privacy Notice

Products

Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence Central

Support

Documentation
Learning Center
Free Support
Premium Support

News

Blog
In The News
Vulnerability Advisories

About

About Wordfence
Careers
Contact
Security
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

□ By checking this box I agree to the terms of service and privacy policy.*

SIGN UP