Chloe Chamberland August 16, 2021

XSS Vulnerability Patched in SEOPress Affects 100,000 sites

On July 29, 2021 the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerability that we discovered in SEOPress, a WordPress plugin installed on over 100,000 sites. This flaw made it possible for an attacker to inject arbitrary web scripts on a vulnerable site which would execute anytime a user accessed the "All Posts" page.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on July 29, 2021. Sites still using the free version of Wordfence will receive the same protection on August 28, 2021.

We initially reached out to the plugin developer on July 29, 2021. After receiving confirmation of an appropriate communication channel the next day on July 30, 2021, we provided the full disclosure details. The vendor quickly acknowledged the report and a patch was released on August 4, 2021 in version 5.0.4.

We strongly recommend updating immediately to the latest patched version of SEOPress, version 5.0.4, if you are currently using a vulnerable version of the plugin.

Description: Stored Cross-Site Scripting via REST-API
Affected Plugin: SEOPress
Plugin Slug: wp-seopress
Affected Versions: 5.0.0 – 5.0.3
CVE ID: CVE-2021-34641
CVSS Score: 6.4 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 5.0.4

SEOPress is a WordPress plugin designed to optimize the SEO of WordPress sites through many different features, like the ability to add SEO meta-data, breadcrumbs, schemas, and more. One feature the plugin implements is the ability to add a SEO title and description to posts, and this can be done while saving edits to a post or via a newly introduced REST-API endpoint.

```
register_rest_route('seopress/v1', '/posts/(?P<id>\d+)/title-description-metas', [
    'methods'             => 'PUT',
    'callback'            => [$this, 'processPut'],
    'args'                => [
        'id' => [
            'validate_callback' => function ($param, $request, $key) {
                return is_numeric($param);
            },
```

Unfortunately, this REST-API endpoint was insecurely implemented. The `permissions_callback` for the endpoint only verified if the user had a valid REST-API nonce in the request. A valid REST-API nonce can be generated by any authenticated user using the rest-nonce WordPress core AJAX action. This meant that any authenticated user, like a subscriber, could call the REST route with a valid nonce, and update the SEO title and description for any post.

```
'permission_callback' => function ($request) {
    $nonce = $request->get_header('x-wp-nonce');
    if ( ! wp_verify_nonce($nonce, 'wp_rest')) {
        return false;
    }

    return true;
```

The payload could include malicious web scripts, like JavaScript, due to a lack of sanitization or escaping on the stored parameters. These web scripts would then execute any time a user accessed the "All Posts" page. As always, cross-site scripting vulnerabilities such as this one can lead to a variety of malicious actions like new administrative account creation, webshell injection, arbitrary redirects, and more. This vulnerability could easily be used by an attacker to take over a WordPress site.

Disclosure Timeline

July 29, 2021 – Initial discovery and analysis of vulnerability. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users. We initiate contact with the plugin vendor.
July 30, 2021 – The vendor confirms the inbox for handling disclosure. We send over full disclosure details.
August 1, 2021 – The vendor confirms they have received the details and will begin working on a fix.
August 4, 2021 – A newly updated version of the plugin is released containing sufficient patches.
August 28, 2021 – Wordfence free users receive firewall rule.

Conclusion

In today's post, we detailed a flaw in SEOPress that granted attackers the ability to inject arbitrary web scripts that could ultimately allow attackers to take over WordPress sites. This flaw has been fully patched in version 5.0.4. We recommend that WordPress users immediately update to the latest version available, which is version 5.0.4 at the time of this publication, if running a vulnerable version of this plugin.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on July 29, 2021. Sites still using the free version of Wordfence will receive the same protection on August 28, 2021.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as this is a vulnerability that can lead to full site takeover.

Click here to join the WordPress Security mailing list and receive vulnerability reports like this the moment they are published.

Comments

2 Comments

Brent *
August 16, 2021
9:37 am

We're still on the latest 4.x version. Been avoiding going to 5.x till all the bugs are worked out. Is this vulnerability affecting 4.x?

Chloe Chamberland *
August 16, 2021
12:36 pm

Hi Brent,

This vulnerability does not affect any versions prior to 5.0.0, so the 4.x versions are not vulnerable to this. Thanks!