Ram Gall

March 31, 2020

Critical Vulnerabilities Affecting Over 200,000 Sites Patched in Rank Math SEO Plugin

On March 23, 2020, our Threat Intelligence team discovered 2 vulnerabilities in WordPress SEO Plugin – Rank Math, a WordPress plugin with over 200,000 installations. The most critical vulnerability allowed an unauthenticated attacker to update arbitrary metadata, which included the ability to grant or revoke administrative privileges for any registered user on the site. The second vulnerability allowed an unauthenticated attacker to create redirects from almost any location on the site to any destination of their choice.

We reached out to the plugin's developer the next day, on March 24, 2020, and received a response within 24 hours. We privately disclosed the full vulnerability details on March 25, 2020, and the plugin developer released a patch on March 26, 2020. We strongly recommend updating to the latest version, 1.0.41.1, as soon as possible as this is considered a critical security issue.

Wordfence Premium customers received a new firewall rule on March 24, 2020, to protect against exploits targeting this vulnerability. Wordfence users still using the free version will receive the rule after thirty days on April 23, 2020.

Description: Privilege Escalation via Unprotected REST API Endpoint
Affected Plugin: WordPress SEO Plugin – Rank Math
Plugin Slug: seo-by-rank-math
Affected Versions: <= 1.0.40.2
CVE ID: CVE-2020-11514
CVSS Score: 10.0 (Critical)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 10.0.41

WordPress SEO Plugin – Rank Math is a WordPress plugin designed to assist with search engine optimization, and it has a number of features to make doing so easier, including the ability to update metadata on posts. In order to add this feature, the plugin registered a REST-API endpoint, `rankmath/v1/updateMeta`, which failed to include a `permission_callback` used for capability checking.

The vulnerable REST route:

```
register_rest_route(
    $this->namespace,
    '/updateMeta',
    [
        'methods'  => WP_REST_Server::CREATABLE,
        'callback' => [ $this, 'update_metadata' ],
        'args'     => $this->get_update_metadata_args(),
    ]
);
```

The endpoint called a function, `update_metadata` which could be used to update the slug on existing posts, or could be used to delete or update metadata for posts, comments, and terms. This endpoint also allowed for updating metadata for users, leading to this critical vulnerability.

The `update_metadata` function:

```
public function update_metadata( WP_REST_Request $request ) {
    $object_id   = $request->get_param( 'objectID' );
    $object_type = $request->get_param( 'objectType' );
    $meta        = $request->get_param( 'meta' );

    $new_slug = true;
    if ( isset( $meta['permalink'] ) && ! empty( $meta['permalink'] ) ) {
        $post     = get_post( $object_id );
        $new_slug = wp_unique_post_slug( $meta['permalink'], $post->ID, $post->post_status, $post->post_type, $post->
        wp_update_post(
            [
                'ID'        => $object_id,
                'post_name' => $new_slug,
            ]
        );
        unset( $meta['permalink'] );
    }

    $sanitizer = Sanitize::get();
    foreach ( $meta as $meta_key => $meta_value ) {
        if ( empty( $meta_value ) ) {
            delete_metadata( $object_type, $object_id, $meta_key );
            continue;
        }

        update_metadata( $object_type, $object_id, $meta_key, $sanitizer->sanitize( $meta_key, $meta_value ) );
    }

    return $new_slug;
}
```

WordPress user permissions are stored in the `usermeta` table, which meant that an unauthenticated attacker could grant any registered user administrative privileges by sending a `$_POST` request to `wp-json/rankmath/v1/updateMeta`, with an `objectID` parameter set to the User ID to be modified, an `objectType` parameter set to `user`, a `meta[wp_user_level]` parameter set to `10`, and a `meta[wp_capabilities][administrator]` parameter set to `1`.

Alternatively, an attacker could completely revoke an existing administrator's privileges by sending a similar request with a `meta[wp_user_level]` parameter and a `meta[wp_capabilities]` parameter set to empty values. Since many sites have a single administrator with a user ID of `1`, this meant that an attacker could lock an administrator out of their own site.

Note that these attacks are only the most critical possibilities. Depending on the other plugins installed on a site, the ability to update post, term, and comment metadata could potentially be used for many other exploits such as Cross-Site Scripting (XSS).

Affected Versions: <= 1.0.40.2
CVE ID: CVE-2020-11515
CVSS Score: 7.4(High)
CVSS Vector: [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:H]
Fully Patched Version: 10.0.41

The WordPress SEO Plugin – Rank Math plugin includes a number of optional modules, including a module that can be used to create redirects on a site. In order to add this feature, the plugin registered a REST-API endpoint, `rankmath/v1/updateRedirection`, which again failed to include a `permission_callback` for capability checking.

The vulnerable REST route:

```
register_rest_route(
    $this->namespace,
    '/updateRedirection',
    [
        'methods'  => WP_REST_Server::CREATABLE,
        'callback' => [ $this, 'update_redirection' ],
    ]
);
```

The endpoint called a function, `update_redirection`, which could be used to create new redirects or modify existing redirects, with an important limitation. The redirect could not be set to an existing file or folder on the server, including the site's main page. This limited the damage to some extent in that, while an attacker could create a redirect from most locations on the site, including new locations, or any existing post or page other than the homepage, they could not redirect visitors immediately upon accessing the site.

The `update_redirection` function:

```
public function update_redirection( WP_REST_Request $request ) {
    $cmb     = new \stdClass;
    $metabox = new \RankMath\Redirections\Metabox;

    $cmb->object_id    = $request->get_param( 'objectID' );
    $cmb->data_to_save = [
        'has_redirect'            => $request->get_param( 'hasRedirect' ),
        'redirection_id'          => $request->get_param( 'redirectionID' ),
        'redirection_url_to'      => $request->get_param( 'redirectionUrl' ),
        'redirection_sources'     => \str_replace( home_url( '/' ), '', $request->get_param( 'redirectionSources' ) )
        'redirection_header_code' => $request->get_param( 'redirectionType' ) ? $request->get_param( 'redirectionType
    ];

    if ( false === $request->get_param( 'hasRedirect' ) ) {
        unset( $cmb->data_to_save['redirection_url_to'] );
    }

    if ( empty( $request->get_param( 'redirectionID' ) ) ) {
        unset( $cmb->data_to_save['redirection_id'] );
    }

    return $metabox->save_advanced_meta( $cmb );
}
```

In order to perform this attack, an unauthenticated attacker could send a `$_POST` request to `rankmath/v1/updateRedirection` with a `redirectionUrl` parameter set to the location they wanted the redirect to go to, a `redirectionSources` parameter set to the location to redirect from, and a `hasRedirect` parameter set to `true`. This attack could be used to prevent access to all of a site's existing content, except for the homepage, by redirecting visitors to a malicious site.

Protecting REST-API Endpoints

The REST-API functionality in WordPress provides great flexibility for plugin developers. Of course, with that flexibility comes great responsibility. If your plugin is using the REST-API, make sure to include a `permission_callback` on any endpoints you don't want to be available to the public, though be aware this also requires that a valid `wp_rest` nonce be generated and sent with any requests to the protected endpoint.

Disclosure Timeline

March 23, 2020 – Wordfence Threat Intelligence discovers and analyzes vulnerabilities.
March 24, 2020– Initial contact with the plugin's developer team. Firewall rule released for Wordfence Premium users.
March 25, 2020 – Plugin developer confirms appropriate inbox for handling discussion. Full vulnerability disclosure sent.
March 26, 2020 – Patched version of plugin released.
April 23, 2020 – Firewall rule becomes available to Wordfence free users.

Conclusion

In today's post, we discussed 2 vulnerabilities caused by unprotected REST API endpoints in the WordPress SEO Plugin – Rank Math plugin. These vulnerabilities have been fully patched in version 10.0.41, and we strongly recommend that all users of this plugin upgrade to the latest version available immediately. Sites running [Wordfence Premium] have been protected against these vulnerabilities since March 24, 2020. Sites running the free version of Wordfence will receive the firewall rule update on April 23, 2020.

Special thanks to the developers of WordPress SEO Plugin – Rank Math for their rapid response and exemplary handling of our disclosure.

Did you enjoy this post? Share it!

Comments

6 Comments

Andrew *
March 31, 2020
9:49 pm

Without wordfence premium plugin how can we solve it?

Ram Gall *
April 1, 2020
8:29 am

Hi Andrew!

If possible, we'll typically wait until a patched version is is available to publicly disclose vulnerabilities. In this case, the Rank Math SEO plugin has been patched, and updating to the latest version should be sufficient to protect your site(s) from these vulnerabilities, even if you're running the free version of Wordfence.

Abdelfatah Aboelghit *
March 31, 2020
11:40 pm

Thanks for the heads up!

SwiftChat Live Chat App *
April 1, 2020
5:30 am

Interesting development. But the good thing is that WP is patched now.

Ngô Văn Cương *
April 3, 2020
8:10 pm

Thanks you very much, I have started to use Wordfence

Rakesh *
April 13, 2020
9:17 am

Thanks a lot for this information

Breaking WordPress Security Research in your inbox as it happens.

you@example.com

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

SIGN UP

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