

🏠 Home :: Critical Information Disclosure on WP Courses plugin exposes private course videos and materials [CVE-2020-26876]

Today we've got an interesting story to share. A vulnerability in WP Courses caused **our java course** to be publicly disclosed via the WordPress REST API. Let's dive into the details and see what happened.

Since version 4.7 of WordPress, the REST API is a default feature. It can be found at URL endpoint `/wp-json/wp/v2`. It will serve all of your websites' content in a JSON structure. That way, external services that want to read data from your website won't have to scrape HTML pages made for human eyes. They just query the REST API.

For reasons of backwards compatibility it's still included with the newest version of WordPress. But efforts are made to have it replaced with the REST API, which doesn't suffer from the same vulnerabilities. Still, we are dealing with an API, so we have:

So far so good. What if we try to get the content via the REST API? WordPress is making it easy for us, by adding a `<link rel="alternate">` tag to its pages.

The link tag is pointing to the REST API endpoint

REST API Handbook

Course video URL leaked to unauthorized users

In WordPress, there is a distinction between pages and posts. A page is content that stays relevant over time, whereas a post is like an article. This distinction has been there since the beginning of WordPress, and it is reflected in the REST API as well: page content can be fetched from `/wp-json/wp/v2/pages`, and posts from... you guessed it right, `/wp-json/wp/v2/posts`.

For WP Courses, a 'page' or a 'post' doesn't really fit nicely the description of course content. They decided instead to create new post types, called 'course', 'lesson', and 'teacher'. Consequently, their content is browsed via REST API endpoint `/wp-`

This may be a good place to introduce yourself and your site or include some credits.

For WP Courses, a 'page' or a 'post' doesn't really fit nicely the description of course content. They decided instead to create new post types, called 'course', 'lesson', and 'teacher'. Consequently, their content is browsed via REST API endpoint `/wp-`

`/wp-json/wp/v2/course`, `/wp-json/wp/v2/lesson` and `/wp-json/wp/v2/teacher` respectively.

Creating new post types

Defining new post types is done via the WordPress method `register_post_type`. As can be seen from the documentation, it takes an array of options. One of them is called `'show_in_rest'`:

• **'show_in_rest'**
(bool) Whether to include the post type in the REST API. Set this to true for the post type to be available in the block editor.

WordPress API documentation of the `register_post_type` function

As you may have guessed by now, WP Courses had set this option explicitly to `'true'`, causing the contents to be accessible via the REST API.

```
373 $args = array(  
374     'show_in_admin_bar' => true,  
375     'menu_icon'         => null,  
376     'show_in_nav_menus' => false,  
377     'publicly_queryable' => true,  
378     'exclude_from_search' => true,  
379     'has_archive'        => false,  
380     'query_var'          => true,  
381     'can_export'         => true,  
382     'rewrite'            => true,  
383     'show_in_menu'       => '',  
384     'has_archive'        => true,  
385     'hierarchical'       => false,  
386     'public'             => true,  
387     'show_ui'            => true,  
388     'hierarchical'       => false,  
389     'labels'             => $labels,  
390     'description'        => __('Enter a lesson description'),  
391     'supports'           => array( 'title', 'editor',  
392                               'show_in_rest' => true,  
393                               ),  
394 );  
register_post_type( 'lesson', $args );
```

From the source code of WP Courses, we can see the `'show_in_rest'` attribute is set to `true` for the post type `'lesson'`.

Setting this option to false solved the issue immediately.

← → 🔍 🌐

https://training.redninemag.com/wp-json/wp/v2/lesson/850

["code":"","test_js_route","message":"No route was found matching the URL and request method","data":{"status":404}}

Preventing exposure of the content via the REST API

Detection of the vulnerability

We were alerted of the vulnerability by looking at log files. A number of different IP addresses were seen to download our course content, without purchasing the course first. We immediately suspected a breach at this point, but the method was yet unclear. The filenames of our videos are hard to guess, and it would take some kind of enumeration vulnerability to find out their paths.

Pretty soon we found out that the `/wp-json/` endpoint was queried more often than usual. It led us to eventually discover the content leak of WP courses via the REST API.

Pirates in sight

Before we could recover from the vulnerability, a number of people have downloaded our course material without paying for it. In other words, it was stolen by purposefully looking for a way to get access to the videos.

In total 38 IPs have been tracked doing that. Many of them are residential IP addresses (both static and dynamic). Some others are business IP addresses or VPS hosted on Amazon, OVH, etc... We've seen people from Myanmar, Mexico, Iran, Peru, Italy, The Netherlands, France, Israel, USA, India, Albania, Egypt, UK, Philippines, Ecuador, Madagascar, Belgium, Estonia, and a place falling under the British crown jurisdiction called 'Isle of Man'. It appears one of the first using this trick was an IP from *"Amazon Technologies Inc"*. It also appears the content has been shared mainly via Telegram.

Our course

We feel it's unfair not to pay for work that has cost us many hours to put together.

We also understand you may not be able to afford it.

Because of the breach and the enormous interest we got from the recent campaign on Twitter, we made the decision to try something different. From today, **the course is available for the excellent price of what you think is fair**.

We urge you - including those who have obtained our course by illegal means - to have a good think about how much the course is worth to you. If this works out well, then we will be selling all future courses according to this price model. Obviously we cannot afford to do that if people pay the bare minimum. If we succeed, we can be the first ones with courses affordable to anyone around the world, regardless of purchasing power.

So, we would like to invite all of you interested in becoming an expert on Java hacking to **sign up for our course**. We are still working on the website, but before end of today the course contents and materials will be back.

We'd like to thank you in advance for the support, and let's see if we can make this model work!

Recovery

Before we finish off, let's spend a few words on how we recovered from the vulnerability. After we discovered the issue, we immediately contacted the developers of WP Courses (CVE-2020-26876). They were quick to fix as a patch was pushed the same evening, but the level of details provided was initially insufficient.

Version 2.0.28 of WP Courses has just been released which includes the option to enable or disable the REST API for courses, lessons and teachers. It is disabled by default.

If you don't know what this means then you probably don't have to worry about it :)

Cheers,

Myles
WP Courses

Copyright © 2020 WP Courses. All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
WP Courses
220 Broadwell Rd
Salt Spring Island, BC V8K1H3
Canada

We made WP Courses developers notice that people could have got confused from the information provided, as in the email above there was no mention this was a security issue. Customers could think version 2.0.28 was just a minor release and decide not to fix soon. As a consequence, all their private courses could have been stolen. The reaction to our considerations was the transmission of a new email and the release of a new version (2.0.29).

An important security update for WP Courses has just been released.

There is a vulnerability which allows for restricted lesson content to be accessed via the REST API. Update now to 2.0.29 to secure this vulnerability.

Sincerely,

Myles
WP Courses

Notification about the availability of a new version of WP Courses plugin

On our side no customer data was leaked during the breach. User names, e-mail addresses and order information are not part of the WP courses plugin, and thus were not at risk.

We assessed the use of the REST API, and disabled it as a preventative measure, even though there could be many legit use cases to keep it enabled.

Of course we are not going to trust WP Courses plugin anymore . Our future courses are probably going to be hosted on other platforms. Stay tuned!

#hacking #information disclosure #javahackingcourse #unauthorized access

#wp-courses

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

☐ Save my name, email, and website in this browser for the next time I comment.

Submit

OUR COURSES

Practical Web Application Hacking – Basic

Practical Web Application Hacking – Advanced

Hacking Java Web and Client Apps (online)

Learning Crypto by defeating Crypto

FIND US

Address
123 Main Street
New York, NY 10001

Hours
Monday—Friday: 9:00AM–5:00PM
Saturday & Sunday: 11:00AM–3:00PM

BLOG CATEGORIES

Binary exploitation

Bug Bounty

Cloud

Courses

Crypto

Docker

Java Hacking

Privilege Escalation

Red Teaming

Reverse engineering

FOLLOW US

Twitter

CONTACT US

Contact form

Email

READ OUR BLOG

IoT/CS Armageddon: hacking devices like there's no tomorrow (part 1)

Challenges in the always moving cloud

The thin line between the cloud provider and the customer applications

When a Denial of Service matters: fighting with risk assessment guys

Bug bounty failure stories to learn from: how we ended up to hack a bank with no reward

