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

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 detai and see what happened.

WordPress REST API

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.

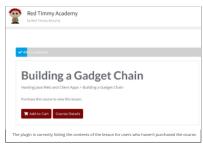
You may be aware of another method, providing similar services: xml-rpc. This entrypoint has been known for being vulnerable to brute-force attacks, and is suggested to be disabled in many articles

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:

- Increased attack surface
 An easier way for attackers to crawl content

The vulnerable plugin: WP Courses

We host our online course using WP Courses. This \$79 plugin (a free version without support for payments is also available) allows you to define courses with lessons. Only when a user is registered to WordPress and has bought the product via WooCommerce,



So far so good. What if we try to get the content via the REST API? WordPress is making it

Let's have a look at what the REST API endpoint exposes. Its behavior is documented in the REST API Handbook of WordPress. It states the following about private content:

The REST API is a developer-oriented feature of WordPress. It provides data access to the content of your site, and implements the same authentication restrictions — content that is public on your site is generally publicly accessible via the REST API, while private content, passwordprotected content, internal users, custom post types, and metadata is only available with authentication or if you specifically set it to be so.

ever, when we browse to our lesson we get the full contents of the page, including the secret link to the course video.

To be clear, this was accessible to unauthenticated users. A registered account on our

How is this possible?

Root cause analysis

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-

Apart from making it easier for attackers to parse content, there is nothing wrong with it being accessed using an API. It's all public content anyways. Then why does 'private'

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 /wpBECOME A JAVA HACKING EXPERT!



as virtual course.

tricks, crypto exploitation and more.

LATEST BLOG POSTS

IoT/ICS Armageddon; hacking devices like there's no tomorrow (part 1)

The thin line between the cloud provider and the customer applications

When a Denial of Service matter

how we ended up to hack a bank with no

Fortinet SIEM vulnerability allows us to get RCE on internet exposed hosts

Critical Information Disclosure on WP videos and materials [CVE-2020-26876]

Pulse Secure Windows Client <9.1.6 (CVE-

A Tale of Escaping a Hardened Docker

BLOG ARCHIVE

See all posts

ABOUT THIS SITE

This may be a good place to introduce yourself and your site or include some n/wp/v2/course, /wp-json/wp/v2/lesson and /wp-json/wp/v2/teacher respec

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

(bool) Whether to include the post type in the REST API. Set this to true for the post

WordPress API documentation of the register_post_type function

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

```
$args = array(
                       dmin bar' => true.
          'show_in_adr
'menu_icon'
          'menu_icon' => null,
'show_in_nav_menus' => false,
          'publicly_queryable' => true,
          'exclude from search' => true,
'has_archive' => false
                                     => false,
          'query_var'
                                     => true,
                                     => true,
381
                                     => true,
          'show in menu'
383
                                     => ''',
                                     => true,
385
                                     => false,
                                     => true,
387
388
                                     => true.
                                     => false,
                            => $labels,
389
          'description' => __('Enter a lesson de
          'supports' => array('title', 'edit
392
       register_post_type( 'lesson', $args );
394
        de of WP Courses, we can see the 'show_in_rest' attribute is set to true
type lesson'
```

Setting this option to false solved the issue immediately.



Detection of the vulnerability

We were alerted of the vulnerability by looking at log files. A number of different IP didresses 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 peole from Myanmar, Mexico, Iran, Peru, Italy, The Netherlands, France, Israel, USA, India, Albania, Egypt, UK, Philippines, Ecuador, Nederlands, France, Is ale, USA, Itilda, Nuellal, Egypt, UK, Fillippines, 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.

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 campagin 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

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

Recovery

Before we finish off, let's spend a few words on how we recovered from the vulnerability. ed 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, Af rights reserved.

Copyright 9 2020 WP Courses, Af rights reserved.

You are receiving this email because you opted in via our website.

Our making address it:

WP Courses

WP Courses

WP Courses

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 militor 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

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

There is a vulnerability which allows for restricted season content to be accessed via the REST API. Update none to 2.0.29 to secure this vulnerability.

Sincerely,
Myles
WP Courses
Notification about the availability of a new version of WP Courses pugin.

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

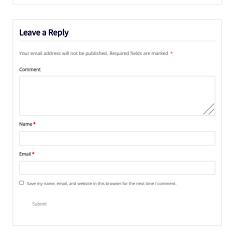
at risk.

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



OUR COURSES Practical Web Application Hacking – Basic Practical Web Application Hacking – Advanced Hacking Java Web and Client Apps (online) Learning Crypto by defeating Crypto Contact form FIND US Address 123 Main Street New York, NY 10001

BLOG CATEGORIES

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

Reverse engineering

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

Cloud Challenges in the always moving cloud

Courses The thin line between the cloud provider and the customer applications

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

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

Red Teaming

READ OUR BLOG

Web Application Hacking