enferas / CVE-2022-34026.md

Created 2 months ago

directory traversal in ICEcoder

CVE-2022-34026.md

directory traversal in ICEcoder https://github.com/icecoder/ICEcoder version 8.1

In file https://github.com/icecoder/ICEcoder/blob/master/lib/settings.php

```
//line 62
if (true === isset($_POST['username']) && "" !== $_POST['username']) {$username = $_
$settingsFile = 'config-' . $username . str_replace(".", "_", str_replace("www.", ""
// line 110
$ICEcoderUserSettings = $settingsClass->getConfigUsersSettings($settingsFile);
```

In file https://github.com/icecoder/ICEcoder/blob/master/classes/Settings.php

```
//line 160
// Note: the source is in the $filename
public function getConfigUsersSettings($fileName)
    {
        // Get users config file details
        $fullPath = $this->getConfigUsersFileDetails($fileName)['fullPath']; // $ful
        $settingsFromFile = $this->serializedFileData("get", $fullPath); // attacker
        // Now return
        return $settingsFromFile;
    }

//line 142
// Note: the source is in the $filename
public function getConfigUsersFileDetails($fileName)
```

```
    {
        // Return details about the users config file
        $fullPath = dirname(__FILE__) . "/../data/" . $fileName;
        $exists = file_exists($fullPath);
        $readable = is_readable($fullPath);
        $writable = is_writable($fullPath);
        $filemtime = filemtime($fullPath);
        return [
            "fileName" => $fileName,
            "fullPath" => $fullPath,
            "exists" => $exists,
            "readable" => $readable,
            "writable" => $writable,
            "filemtime" => $filemtime,
        ];
    }

// line 226
public function serializedFileData($do, $fullPath, $output=null)
    {
        if ("get" === $do) {
            if (function_exists('opcache_invalidate')) {
                opcache_invalidate($fullPath, true);
            }
            $data = file_get_contents($fullPath); // Note: $fullPath is controlled b
            $data = str_replace("<"."?php\n/*\n\n", "", $data);
            $data = str_replace("\n\n*/\n?".">", "", $data);
            $data = unserialize($data);
            return $data;
        }
        if ("set" === $do) {
            if (true === is_array($output)) {
                $output = serialize($output);
            }
            return false !== file_put_contents($fullPath, "<"."?php\n/*\n\n" . $outp
        }
    }
```

CVE-2022-34026 is assigned to this report.