New issue

Possible XSS Vulnerability #2252

⊘ Closed   **enferas** opened this issue on Jun 6 · 6 comments

---

Labels   bug   security   Solved

---

enferas commented on Jun 6

Hello,

I would like to report for possible XSS vulnerability.

In file https://github.com/serghey-rodin/vesta/blob/master/web/api/v1/upload/UploadHandler.php

the source in function post

```
    public function post($print_response = true) {
        //....
        // the source $_FILES[$this->options['param_name']]
        $upload = isset($_FILES[$this->options['param_name']]) ? $_FILES[$this->options['param_name']]
        // ....
        foreach ($upload['tmp_name'] as $index => $value) {
            // $files will have the source which return from handle_file_upload
            $files[] = $this->handle_file_upload(
                $upload['tmp_name'][$index],
                $file_name ? $file_name : $upload['name'][$index],
                $size ? $size : $upload['size'][$index],
                $upload['type'][$index], // The source
                $upload['error'][$index],
                $index,
                $content_range
            );
        }
        //.....
        // call generate_response and pass the source in the array in $files
        return $this->generate_response(
            array($this->options['param_name'] => $files),
            $print_response
        );
    }
```

function handle_file_upload

```
    protected function handle_file_upload($uploaded_file, $name, $size, $type, $error,
        //.....
        // the source in $file->type
        $file->type = $type;
        //....
        return $file;
    }
```

function generate_response

```
    protected function generate_response($content, $print_response = true) {
        if ($print_response) {
            $json = json_encode($content);
            //.....
            $this->body($json);
        }
    }
```

Finally, the sink in function body

```
  protected function body($str) {
        // the sink
        echo $str;
    }
```

byjameson commented on Jun 10

yes this is bug

myvesta commented on Jun 15

Can you check is this issue exists in https://github.com/myvesta/vesta fork?

↗ This was referenced on Jul 2

CRITICAL - Vesta is no longer supported - Suggested easy migration #2254

⊘ **Closed**

vesta-php.sock #2255 `Closed`

---

jaapmarcus commented on Jul 19   `Contributor`

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36305

---

anton-reutov commented on Jul 22   `Collaborator`

📖 Possible XSS Vulnerability

🏷️ ⊙ **anton-reutov** added   bug   security   labels on Jul 22

↗️ **divinity76** added a commit to divinity76/vesta that referenced this issue on Jul 23

  🖼️ fix xss / `serghey-rodinGH-2252` …   0682f7b

↗️ 🖼️ **divinity76** mentioned this issue on Jul 23

fix xss / GH-2252 #2258

`⑆ Merged`

---

divinity76 commented on Jul 23   `Contributor`

proposed a fix: #2258

fwiw VestaCP development has largely halted, notable maintained forks are
https://github.com/hestiacp/hestiacp and https://github.com/myvesta/vesta

❤️ 1

↗️ ⊙ **anton-reutov** added a commit that referenced this issue on Jul 27

  ⊙ Merge pull request **#2258** from divinity76/patch-5 …   51e468c

---

🏷️ ⊙ **anton-reutov** added the   Solved   label on Jul 27

---

anton-reutov commented on Jul 27   `Collaborator`

Thank you guys for the help

anton-reutov closed this as completed on Jul 27

Assignees

No one assigned

Labels

bug   security   Solved

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants