Stored XSS via SVG File in inventree/inventree

0

Valid Reported on Sep 16th 2022

Description

By uploading SVG files, the users can perform Stored XSS attack.
Copy the following code and save as filename.svg.

Proof of Concept

```
<x:script xmlns:x="http://www.w3.org/1999/xhtml">alert(document.domain)</x:
```

[1] Login as user with upload permission.
[2] upload the payload injected SVG file at https://demo.inventree.org/order/sales-order/3/
[3] Copy the uploaded svg file url and open in new tab. (every logged user can access to this url)
[4] XSS ! (https://demo.inventree.org/media/so_files/3/yourfile.svg)
if you need more specific information, feel free to contact me.

Impact

If an attacker can execute the script in the victim's browser via SVG file, they might compromise that user by stealing its cookies.

CVE
CVE-2022-3355
(Published)

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

Severity
High (8.2)

Registry
Other

Affected Version

0.9.0 dev

Visibility
Public

Status
Fixed

Found by

Hakiduck

@mike993

pro

This report was seen 888 times.

We are processing your report and will contact the **inventree** team within 24 hours.
2 months ago

Hakiduck modified the report 2 months ago

We have contacted a member of the **inventree** team and are waiting to hear back 2 months ago

Matthias Mair validated this vulnerability 2 months ago

Thank you for your report @mike993! Do you have a suggestion for good svg validation in Django?

Hakiduck has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Hakiduck 2 months ago Researcher

in my experience, i used these two libraries:

https://github.com/mattkrick/sanitize-svg (easier, with example client and server side)

https://github.com/clones/html5lib/blob/master/python/src/html5lib/sanitizer.py (can be used also with html tag)

I hope I was helpful.

Matthias Mair 2 months ago Maintainer

@mike993 thanks for the hints, a possible fix is being reviewed now.

We have sent a fix follow up to the **inventree** team. We will try again in 7 days. 2 months ago

Matthias Mair marked this as fixed in 0.8.3 with commit 5a08ef 2 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Hakiduck 2 months ago Researcher

@admin could we get CVE?

Jamie Slome 2 months ago Admin

Happy to assign a CVE once we get the go-ahead from the maintainer 👍

Matthias Mair 2 months ago Maintainer

@admin go-ahead from my side for a CVE. The fix is released and already deployed on the bigger deployments

Jamie Slome 2 months ago Admin

Sorted :)

Sign in to join this conversation