Cross-site Scripting (XSS) - Stored in django-helpdesk/django-helpdesk

0

Valid Reported on Nov 11th 2021

Description

Stored XSS via upload 'Attachments' with format .svg or .html

Detail

When opening the attachment, some format files will be rendered and loaded on the browser. So it allows executing arbitrary javascript code that was injected into attachment before.

Proof of Concept

```
// PoC.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">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;s
   <script type="text/javascript">
      alert("XSS");
   </script>
</svg>
```

Step top Reproduct

Create a ticket with an unauthenticated user
Upload .svg or .html into attachments
The XSS will trigger when the admin open the attachment

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

References

- Stored Cross Site Scripting

CVE
CVE-2021-3950
(Published)

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

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

lethanhphuc
@noobpk
unranked

Fixed by

lethanhphuc
@noobpk
unranked

This report was seen 369 times.

We are processing your report and will contact the **django-helpdesk** team within 24 hours.
a year ago

We have contacted a member of the **django-helpdesk** team and are waiting to hear back
a year ago

Garret Wassermann validated this vulnerability a year ago

lethanhphuc has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

lethanhphuc submitted a **patch** a year ago

lethanhphuc a year ago Researcher

PR: https://github.com/django-helpdesk/django-helpdesk/pull/984

Garret Wassermann marked this as fixed with commit **04483b** a year ago

lethanhphuc has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome a year ago Admin

CVE published! 🎉

Sign in to join this conversation