New issue

Jump to bottom

Transfer.sh Vulnerable to Stored XSS #500

Closed **blind-intruder** opened this issue on Aug 11 · 0 comments

blind-intruder commented on Aug 11 Contributor

Hi,
I am Farhan, a professional cyber security researcher & penetration tester from Pakistan. I was reviewing the code of the transfer.sh and I found that it is possible to achieve Cross Site Scripting (XSS) on transfer.sh.

Steps to Reproduce:

- Create a file without any extension, example: "poc"
- Add this HTML in this file " `<h3 onclick="alert('XSS')">click me</h3>` "
- Save this file
- Upload this file in the transfer.sh
- You will get a url something like this: https://transfer.sh/OHTwGK/poc
- Modify this url and add "inline" just after https://transfer.sh/
- Now the url will look like this: https://transfer.sh/inline/OHTwGK/poc
- Open this url in browser and click on the "click me" text and notice the prompt

How to Fix it:
In the file /server/handlers.go find this code: line # 1035:
https://github.com/dutchcoders/transfer.sh/blob/main/server/handlers.go#L1035

```
if action == "inline" {
      disposition = "inline"
}
```

Replace this code with the following to add proper content type:

```
if action == "inline" {
      disposition = "inline"
      contentType := "text/plain"
}
```

Proof Of Concept:
Open the following url and click on the "click me" text and you will see an alert popup, which confirms XSS.
https://transfer.sh/inline/OHTwGK/poc

aspacca closed this as completed on Sep 11

GoVulnBot mentioned this issue on Sep 29

x/vulndb: potential Go vuln in github.com/dutchcoders/transfer.sh: CVE-2022-40931
golang/vulndb#1030

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants