

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

✓ Valid

Reported on Feb 8th 2022

Description

Stored XSS in parameter 'host' when add server

Proof of Concept

[illegible]

Step to Reproduct

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

-  serversList.php L47-L49
-  main.php L80
-  serversList.php L72
-  main.php L68

CVE
CVE-2022-0539
(Published)


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

Severity
Medium (6.3)

Visibility
Public

Status
Fixed

Found by




lethanhphec

@noobpk

unranked ▼

Fixed by



lethanhphec

@noobpk

unranked ▼

Chat with us

This report was seen 337 times.

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 ✗

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

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us