huntr

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

1



Reported on Jan 31st 2022

Description

Beanstalk Console is vulnerable to reflected Cross-Site Scripting via the server parameter.

Steps to reproduce

Setup the Beanstalk console locally.

Go to https://localhost/public/? and add a random server.

Visit https://localhost/public/?server=%3Cimg%20src=x%20onerror=alert(document.domain)%3E

You can see that an alert pops up with the domain name confirming the reflected XSS

Occurrences



nclude.php L22

CVE

Vulnerability Type

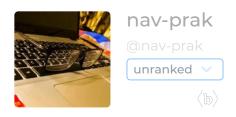
Severity

Visibility

Status

Found by

Chat with us







This report was seen 390 times.

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

We created a GitHub Issue asking the maintainers to create a SECURITY.md 10 months ago

We have contacted a member of the **ptrofimov/beanstalk_console** team and are waiting to hear back 10 months ago

ptrofimov 10 months ago

Maintainer

I am a collaborator on the repo, and I am checking now the details.

nav-prak submitted a patch 10 months ago

nav-prak 10 months ago

Researcher

Do let me know if more information is required to verify the issue

We have sent a follow up to the **ptrofimov/beanstalk_console** team. We will try again in 7 days. 10 months ago

ptrofimov validated this vulnerability 10 months ago

nav-prak has been awarded the disclosure bounty 🗸

Chat with us

The fix bounty is now up for grabs

ptrofimov marked this as fixed in 1.7.12 with commit e351c8 10 months ago
nav-prak has been awarded the fix bounty ✓
This vulnerability will not receive a CVE 🗶
include.php#L22 has been validated ✓

Sign in to join this conversation

2022 © 418sed

-	h	1.1	\mathbf{r}		+	r
-	ш	ч	н	ı	L	ı,

home

hacktivity

leaderboard

FAO

contact us

terms

privacy policy

part of 418sec

company

about

team