huntr

Arbitrary Command Injection in strapi/strapi

1

✓ Valid Reported on Feb 17th 2022

Description

When creating a strapi app using npxcreate-strapi-app, we can inject arbitrary commands through the template cli argument as per the code in this particular link (https://github.com/strapi/strapi/blob/master/packages/generators/app/lib/utils/fetch-npm-template.js#L13), this happens due to improper sanitization of user input.

Steps to Reproduce the POC

```
1) npx create-strapi-app my-project --quickstart --template ";touch poc.txt
2) Perform "ls" command and you will see that a file called "poc.txt" was c
```

Impact

An attacker can execute arbitrary os commands which can help him perform local privilege escalation to gain root access if strapi package can be run as sudo.

PoC (Proof)

https://prnt.sc/26xuo5z

Fix / Solution

Sanitize the input of template parameter before introducing it to the execution context.

Regards,
R.Srikar (zeltronsrikar@gmail.com) & Abhishek S(abhiabhi2306@gmail.com)

References

- CWE-78

- CWE-78

CVE

CVE-2022-0764
(Published)

Vulnerability Type
CWE-78: OS Command Injection

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

231tr0n
@231tr0n
unranked

This report was seen 957 times.

We are processing your report and will contact the **strapi** team within 24 hours. 9 months ago

We have contacted a member of the **strapi** team and are waiting to hear back 9 months ago

We have sent a follow up to the **strapi** team. We will try again in 7 days. 9 months ago

Alexandre BODIN 9 months ago Maintainer

@admin, This issue is accurate but the severity doesn't really make sense as most of the time the only person that can use this vector is the developer running the command themselves on their computer. We are going to make a fix for the sake of it but it is far from being critical

Jamie Slome 9 months ago Admin

@alexandrebodin - thank you for the information here!

Chat with us

You are welcome to adjust the severity of the report using the `adjust severity` button on the action buttons in the right panel.

Let me know if you have any questions!

Alexandre BODIN modified the report 9 months ago

Alexandre BODIN validated this vulnerability 9 months ago

231tr0n has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Alexandre BODIN 9 months ago Maintainer

@admin it's a bit unclear where do we put the fix info. It wasn't fixed but the reporting person so not sure we should use the confirm fix button here. Can you walk me through that please

Jamie Slome 9 months ago Admin

@alexandrebodin - if you click the `Confirm fix` button, a modal will pop up asking about the branch and commit SHA that the fix exists on/at (it does not confirm a fix immediately). You will also be able to select who the fixer is too. Once you have filled this information in, you can submit the form.

Let me know if you have any more questions!

Alexandre BODIN marked this as fixed in 4.1.0 with commit 2a3f5e 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us