11

Denial Of Service in Strapi Framework using argument injection

Share:

TIMELINE

princechaddha submitted a report to Node.js third-party modules. Jan 5th (3 years ago)

I would like to report Denial Of Service in Strapi Framework.It allows attacker to force restart the server using argument injection.

Module

module name: strapi
version: 3.0.0-beta.18.3 and earlier
npm page: `https://www.npmjs.com/package/strapi`

Module Description

> The Strapi HTTP layer sits on top of Koa. Its ensemble of small modules work together to provide simplicity, maintainability, and structural conventions to Node.js applications.

Module Stats

[1] weekly downloads 8,508

Vulnerability

Vulnerability Description

> While reviewing source code i found that "installPlugin" and "uninstallPlugin" handler functions for the admin panel (https://github.com/strapi/strapi/blob/master/packages/strapi-admin/controllers/Admin.js) is using regex on line 70 & 110 i.e `/^[A-Za-z0-9_-]+$/` before passing user input to `execa()` on line 77 & 117 to prevent command injection but the regex allows `-` character.Using this attacker can pass valid arguments like "-h" "-v" "--help" which will add after the command `npm run strapi -- install <user-input>` & `npm run strapi -- uninstall <user-input>` and leads the serve to restart.

Steps To Reproduce:

> Create a new strapi project and start the server by using yarn.
> Login to admin panel by visiting http://172.16.129.155:1337/admin/
> Goto http://172.16.129.155:1337/admin/marketplace & click on download while intercepting the request.
> Change value of plugin to "-h", "--help", "-v" or "--version"
> Check console the server will restart everytime we send the request using valid strapi arguments.

Patch

> Instead of `strapi.reload();` after executing the command there should be a check to validate if a valid plugin is installed or uninstalled.Many user uses `_` & `-` in plugin names so blacklisting the above 4 inputs will fix this issue instead of removing `_` & `-` from the regex

Wrap up

> Select Y or N for the following statements:

- I contacted the maintainer to let them know: [Y/N] N
- I opened an issue in the related repository: [Y/N] N

Also, It looks like an intented behaviour to restart server after uninstalling or installing a valid plugin but by just passing the valid arguments we can restart the server.

Impact

Attacker can cause the server to restart even without installing or uninstalling a valid plugin.

vdeturckheim Node.js third-party modules staff posted a comment. Jan 6th (3 years ago)

Hello @princechaddha ,
Thanks for this report.

This looks like a low impact to me (the attacker needs to be able to login to admin first and restarting the server is the normal behavior for Strapi when a plugin is installed). But IMO this still is a problematic bug in Strapi.

I am in touch with Strapi's CTO and will invite him to join this report.

Vlad

vdeturckheim Node.js third-party modules staff changed the status to Triaged. Jan 6th (3 years ago)

vdeturckheim Node.js third-party modules staff updated the severity to Low (2.7). Jan 6th (3 years ago)

strapi joined this report as a participant. Jan 6th (3 years ago)

strapi posted a comment. Jan 6th (3 years ago)

Hi,

Thanks for reporting this issue. We will make some changes to make sure this cannot happen. a Simple regex change to check it doesn't start by a - or a -- will do the trick as there are no npm dependencies that can start with a -.

Other note: this cannot happen in production. The reload is only happening in development mode ;)

princechaddha posted a comment. Jan 7th (3 years ago)

Hey @vdeturckheim @strapi @tabascojellybeans, can i get CVE for this issue ? I know the severity is low but attacker was able to inject argument in strapi via admin panel.

vdeturckheim Node.js third-party modules staff posted a comment. Jan 7th (3 years ago)

@princeofpersia right now, I'd like to postpone the CVE assignment until Strapi team has a fix. It does not seem to me that there is an urgent need for publicizing it as it requires admin access and only work in development mode. Wdyt?

princechaddha posted a comment. Updated Jan 7th (3 years ago)

Yes it is not urgent i was just asking if this can get a CVE.I will also check the production mode tonight.
Also thanks for giving credit to h1 triagger @princeofpersia instead of @princechaddha. May be he will mark my N/A as triaged in future for a CVE 🔥 😂
As everyone on twitter is bashing CVE's right now #infosecdrama 🌜

vdeturckheim Node.js third-party modules staff posted a comment. Jan 7th (3 years ago)

@princechaddha sorry about the nickname mix :facepalm:. Autocompletion got me here. I can assure you the CVE will be for you when published ;)

strapi posted a comment. Jan 7th (3 years ago)

FYI fix released in v3.0.0-beta.18.4

princechaddha posted a comment. Jan 8th (3 years ago)

Yes the fix `https://github.com/strapi/strapi/commit/c0c191c08f05fe10d7a6b1bf9475c1a651a89362` looks good to me but the plugin name can even starts with a number like `247test` you have restricted the first letter to be an alphabet.
The regex should be `/^[A-Za-z0-9][A-Za-z0-9-_]+$/` but thats up to you.

vdeturckheim Node.js third-party modules staff posted a comment. Jan 13th (3 years ago)

@strapi what do you yhink here? Is it good to publish this bug for you?

strapi posted a comment. Jan 13th (3 years ago)

@princechaddha Actually the name is always prefixed when running the install command because the names are only packages published by us. With no numbers in it ;)

@vdeturckheim Sure can be published. Thank you !

vdeturckheim Node.js third-party modules staff closed the report and changed the status to **Resolved**. Jan 27th (3 years ago)

vdeturckheim Node.js third-party modules staff requested to disclose this report. Jan 27th (3 years ago)

princechaddha agreed to disclose this report. Jan 28th (3 years ago)

This report has been disclosed. Jan 28th (3 years ago)