



Thank you for contacting the npm security team. Vulnerabilities in npm packages should be reported directly to the package maintainers. A link to the associated repository where you can file an issue can likely be found on the package page on npmjs.com. You can also find their contact information with npm owner 1s. spackage-names.

If the package contains malicious code please provide more details and we will ensure it is removed from the npm registry and users cannot be affected.

We really appreciate your report. Please let us know if there's anything else we can help with.





收件人: quitlahok@gmail.com; ruyadorno@hotmail.com; Darcy Clarke <darcy@darcyclarke.me>; i@izs.me;

I would like to report a Regular Expression Denial of Service (REDoS) vulnerability in ssri.

It allows cause a denial of service when parsing crafted invalid SRI strings.

You can execute the code below to reproduce the vulnerability

const ssri = require('ssri')

// reasing and senaring // const parsed = ssri.parse(integrity) const parsed = ssri.parse(integrity, ("strict":true, "single":true}) ssri.stringify(parsed) // === integrity (works on non-Integrity objects) var s = parsed.toString() // === integrity

console.log(s)

Best. Yeting Li





I apologize for the delayed response. Your report shouldn't have been turned away originally from our Support/Security Triage & I apologize for that confusion. Our team (ie. npm CLI Team) is looking into this right now & we'll make sure to give you an update when we've got a patch ready or released. Appreciate you bringing this to our attention & again apologize for the back-&-forth you went through.

Expect me to follow up here in the next few days. If you don't hear from me by the end of the week, feel free to email me directly again.

Darcy Clarke

http://twitter.com/dancy http://github.com/darcyclarke https://angel.co/darcyclarke http://ca.linkedin.com/in/darcyclarke +1 647 382 3022