

Hi,

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 cpackage-name>

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.



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')
   //\ const\ integrity = \ 'sha512-9KhgCRIx/AmzC8xqYJTZRrnO8OW2Pxyl2DIMZSBOr0oDvtEFyht3xpp71j/r/pAe1DM+JI/A+line3jUBgzQ7A==?foo'' and the constant of the cons
 // Parsing and serializing
 // const parsed = ssrl.parse(integrity)
const parsed = ssrl.parse(integrity,("strict":true,"single":true))
 ssri.stringify(parsed) // === integrity (works on non-Integrity objects)
var s = parsed.toString() // === integrity
console.log(s)
```



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

Hi.

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')

 $// const integrity = {}^{i}sha512-9KhgCRIx/AmzC8xqYJTZRrnO8OW2Pxyl2DIMZSBOr0oDvtEFyht3xpp71j/r/pAe1DM+JI/A+line3jUBgzQ7A==?foo'} \\$ 

// Parsing and serializing

// 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



标记为来

Her 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.

Cheers Darcy

Darcy Clarke

www.darcyclarke.me www.darcyclarke.me http://withc.com/darcyclarke https://ajthub.com/darcyclarke https://angel.co/darcyclarke http://ca.linkedin.com/in/darcyclarke +1.647.382.3022



收件人: Darcy Clarke <darcy@darcyclarke.me>;

Hi Darcy,

I hope you are all well.

How's it going now about the disclosure?

Best, Yeting

ReDoS in ssri



We've queued up a patch & will be pushing out this update in our next release (should be Thursday): https://github.com/npm/ssri/pull/17

I saw that you've also found an issue in hosted-git-info, I'll make sure we look into that right away as well & try to release a fix at the same time. Appreciate the disclosures &, as mentioned before, in the future, we hope you can use &/or submit issues via `security@npmjs.com` that will get directed to our team internally if they're for packages own.

标记为未

Cheers, Darcy

P.S. I'll follow up in the other email thread with updates for hosted-git-info

Darcy Clarke

www.darcyclarke.me http://wittar.com/darcy http://github.com/darcyclarke https://angel.co/darcyclarke http://ca.linkedin.com/in/darcyclarke +1 647 382 3022

\* This email may contain confidential information and any rights to privilege have not been waive