Cubic catastrophic backtracking (ReDoS) in `block.def`

High **UziTech** published **GHSA-rrrm-qjm4-v8hf** on Jan 14

Package

marked (npm)

Affected versions	Patched versions
< 4.0.9	4.0.10

Description

Impact

What kind of vulnerability is it?

Denial of service.

The regular expression `block.def` may cause catastrophic backtracking against some strings.
PoC is the following.

```
import * as marked from "marked";

marked.parse(`[x]:${' '.repeat(1500)}x ${' '.repeat(1500)} x`);
```

Who is impacted?

Anyone who runs untrusted markdown through marked and does not use a worker with a time limit.

Patches

Has the problem been patched?

Yes

What versions should users upgrade to?

4.0.10

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

Do not run untrusted markdown through marked or run marked on a worker thread and set a reasonable time limit to prevent draining resources.

References

Are there any links users can visit to find out more?

- https://marked.js.org/using_advanced#workers
- https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS

For more information

If you have any questions or comments about this advisory:

- Open an issue in marked

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-21680

Weaknesses

CWE-400 CWE-1333

Credits

makenowjust