ReDoS vulnerability in Sec-WebSocket-Extensions parser

High **jcoglan** published **GHSA-g78m-2chm-r7qv** on Jun 2, 2020

Package

websocket-extensions (npm)

Affected versions	Patched versions
< 0.1.4	0.1.4

Description

Impact

The ReDoS flaw allows an attacker to exhaust the server's capacity to process incoming requests by sending a WebSocket handshake request containing a header of the following form:

```
Sec-WebSocket-Extensions: a; b="\c\c\c\c\c\c\c\c\c\c ...
```

That is, a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. The parser takes exponential time to reject this header as invalid, and this will block the processing of any other work on the same thread. Thus if you are running a single-threaded server, such a request can render your service completely unavailable.

Patches

Users should upgrade to version 0.1.4.

Workarounds

There are no known work-arounds other than disabling any public-facing WebSocket functionality you are operating.

References

- https://blog.jcoglan.com/2020/06/02/redos-vulnerability-in-websocket-extensions/

Severity

High

CVE ID

CVE-2020-7662

Weaknesses

No CWEs