


ReDoS in Sec-WebSocket-Protocol header

Moderate lpinca published GHSA-6fc8-4gx4-v693 on May 25, 2021

Package

 **ws** (npm)

Affected versions

`>= 5.0.0 < 5.2.3, >= 6.0.0 < 6.2.2, >= 7.0.0 < 7.4.6`

Patched versions

`5.2.3, 6.2.2, 7.4.6`

Description

Impact

A specially crafted value of the `Sec-WebSocket-Protocol` header can be used to significantly slow down a ws server.

Proof of concept

```
for (const length of [1000, 2000, 4000, 8000, 16000, 32000]) {
  const value = 'b' + ' '.repeat(length) + 'x';
  const start = process.hrtime.bigint();

  value.trim().split(/ *, */);

  const end = process.hrtime.bigint();

  console.log(`length = ${length}, time = ${end - start} ns`);
}
```

Patches

The vulnerability was fixed in ws@7.4.6 ([00c425e](#)) and backported to ws@6.2.2 ([78c676d](#)) and ws@5.2.3 ([76d47c1](#)).

Workarounds

In vulnerable versions of ws, the issue can be mitigated by reducing the maximum allowed length of the request headers using the `--max-http-header-size=size` and/or the `maxHeaderSize` options.

Credits

The vulnerability was responsibly disclosed along with a fix in private by [Robert McLaughlin](#) from University of California, Santa Barbara.

References

- [GHSA-6fc8-4gx4-v693](#)
- <https://nvd.nist.gov/vuln/detail/CVE-2021-32640>
- [00c425e](#)
- [#1895](#)

Severity

Moderate

CVE ID

CVE-2021-32640

Weaknesses

CWE-400

Credits

 [robmc14](#)