The If Works

by James Coglan

ReDoS vulnerability in websocket-extensions

On 1 June 2020 it was reported to me that a regular expression denial of service (ReDoS) vulnerability exists in the `websocket-extensions` npm package. This vulnerability was discovered by Robert McLaughlin and has been assigned the identifier CVE-2020-7662.

In the course of investigating this issue I discovered that the Ruby version of `websocket-extensions` contains the same flaw. The vulnerability in this version has been assigned the identifier CVE-2020-7663.

To mitigate this issue, you should install one of these packages as appropriate for your system:

- version 0.1.4 of the npm package
- version 0.1.5 of the rubygems package

All previous versions of these packages are vulnerable.

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.

I would like to thank Snyk for reporting this issue to me, and my employer dxw for giving me time to fix it.

Posted on June 2, 2020. This entry was posted in Faye, JavaScript, Ruby. Bookmark the permalink.

← Controlling mutation with types

→ Missing TLS certificate verification in Faye