yahoo / **serialize-javascript** Public

Code Issues 33 Pull requests 11 Actions Projects Security and qua

Commit `f27d65d`

rrdelaney authored on Jan 9, 2024 Verified

```
fix: serialize URL string contents to prevent XSS (#173)
```

main (#173) · v7.0.5 ••• v6.0.2

1 parent 02499c0 commit f27d65d

2 files changed +5 -3

Top

Filter files…

index.js

test/unit

serialize.js

Search within code

index.js

```
@@ -258,7 +258,7 @@ module.exports = function serialize(obj, options) {
258 258           }
259 259
260 260           if (type === 'L') {
261     -             return "new URL(\"" + urls[valueIndex].toString() + "\")";
    261 +             return "new URL(" + serialize(urls[valueIndex].toString(), options)
      + ")";
262 262           }
263 263
264 264           var fn = functions[valueIndex];
```

test/unit/serialize.js

```
@@ -461,8 +461,8 @@ describe('serialize( obj )', function () {
461 461         describe('URL', function () {
462 462             it('should serialize URL', function () {
463 463                 var u = new URL('https://x.com/')
464     -               expect(serialize(u)).to.equal('new URL("https://x.com/")');
465     -               expect(serialize({t: [u]})).to.be.a('string').equal('{"t":[new URL("https://x.com/")]}');
    464 +               expect(serialize(u)).to.equal('new URL("https:\\u002F\\u002Fx.com\\u002F")');
    465 +               expect(serialize({t: [u]})).to.be.a('string').equal('{"t":[new URL("https:\\u002F\\u002Fx.com\\u002F")]}');
466 466             });
467 467
468 468             it('should deserialize URL', function () {
@@ -477,6 +477,8 @@ describe('serialize( obj )', function () {
477 477
                 expect(serialize('</script>')).to.equal('"\\u003C\\u002Fscript\\u003E"');
478 478                 expect(JSON.parse(serialize('</script>'))).to.equal('</script>');
479 479                 expect(eval(serialize('</script>'))).to.equal('</script>');
    480 +               expect(serialize(new URL('x:</script>'))).to.equal('new URL("x:\\u003C\\u002Fscript\\u003E")');
    481 +               expect(eval(serialize(new URL('x:</script>'))).href).to.equal('x:</script>');
480 482             });
481 483         });
482 484
```

Comments 0

Please sign in to comment.