Code injection using \u005c #99

New issue

Closed **vogelsgesang** opened this issue on 5 Apr 2015 · 2 comments

vogelsgesang commented on 5 Apr 2015 Contributor

Arbitrary JS code can be injected into the output of the `Messageformat.compile` function using the escape sequence `\u005c` (unicode code point for a backslash).

Working example:

```
var MessageFormat = require('./lib/messageformat');
var mf = new MessageFormat('en', null);

var injectionString = "\\u005c{VAR} + console.log('Out of the box'); \\}//";
var test = mf.compile(injectionString);

console.log(test({VAR: 'value'}));
```

vogelsgesang added a commit to vogelsgesang/messageformat.js that referenced this issue on 5 Apr 2015

`regression test for messageformat#99 (failing)` ... `40a583b`

vogelsgesang added a commit to vogelsgesang/messageformat.js that referenced this issue on 5 Apr 2015

`fixes messageformat#99: Code injection using \u005c` `90191f8`

vogelsgesang added a commit to vogelsgesang/messageformat.js that referenced this issue on 5 Apr 2015

`fixes messageformat#99: Code injection using \u005c` `454dfb0`

vogelsgesang mentioned this issue on 5 Apr 2015

Escape sequence for a literal backslash #101 Merged

eemeli closed this in `5d21ef6` on 6 Apr 2015

eemeli commented on 6 Apr 2015 Member

@ericf, is this something to which yahoo/intl-messageformat-parser might also be vulnerable?

ericf commented on 8 Apr 2015

@eemeli this is the AST from intl-messageformat-parser:

```
{
  "type": "messageFormatPattern",
  "elements": [
    {
      "type": "messageTextElement",
      "value": "\\"
    },
    {
      "type": "argumentElement",
      "id": "VAR",
      "format": null
    },
    {
      "type": "messageTextElement",
      "value": " + console.log('Out of the box'); }//"
    }
  ]
}
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Linked pull requests
Successfully merging a pull request may close this issue.
None yet

3 participants