9 Prototype pollution in dot-prop

Share:

TIMELINE

aaron_costello submitted a report to **Node.js third-party modules**. Oct 22nd (3 years ago)

I would like to report a parameter pollution in dot-prop

It allows an attacker to modify the prototype of a base object which can vary in severity depending on the implementation (DoS, access to sensitive data, RCE).

Module

module name: dot-prop
version: 5.1.1
npm page: https://www.npmjs.com/package/dot-prop

Module Description

Get, set, or delete a property from a nested object using a dot path

Module Stats

weekly downloads:
8,627,892

Vulnerability

Vulnerability Description

See previous description

Steps To Reproduce:

Code 178 Bytes Wrap lines Copy Download

```
var dotProp = require("dot-prop")
const object = {};
console.log("Before " + object.b); //Undefined
dotProp.set(object, '__proto__.b', true);
console.log("After " + {}.b); //true
```

Wrap up

> Select Y or N for the following statements:

- I contacted the maintainer to let them know: N
- I opened an issue in the related repository: N

Impact

Can result in: dos, access to restricted data, rce (depends on implementation)