Prototype Pollution

Affecting madlib-object-utils package, versions <0.1.7

INTRODUCED: 14 AUG 2020 CVE-2020-7701 CWE-1321 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `madlib-object-utils` to version 0.1.7 or higher.

Overview

madlib-object-utils is an A small set of utility functions for working with objects

Affected versions of this package are vulnerable to Prototype Pollution via `setValue` .

POC:

```
const objectUtils = require("madlib-object-utils"); objectUtils.setValue('__proto__.polluted', {}, true);
console.log(polluted);
```

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Availability	HIGH

See more

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Prototype Pollution vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-MADLIBOBJECTUTILS-598676
Published	14 Aug 2020
Disclosed	14 Aug 2020
Credit	Beomjin Lee

Report a new vulnerability | Found a mistake?