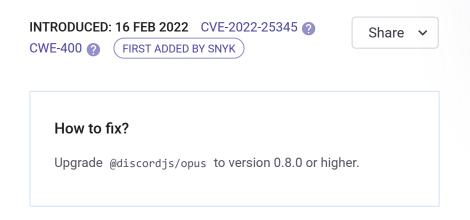
## **snyk** Vulnerability DB

Snyk Vulnerability Database > npm > @discordjs/opus

Q Search by package n

### **Denial of Service (DoS)**

Affecting @discordjs/opus package, versions <0.8.0



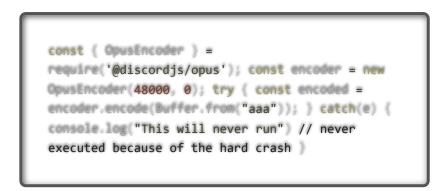
### Overview

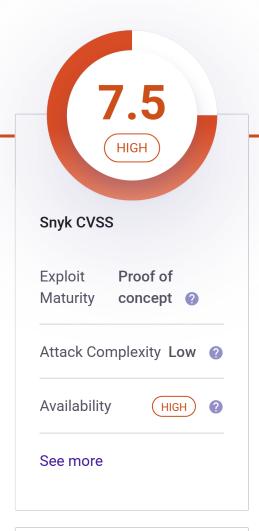
@discordjs/opus is a native bindings to libopus.

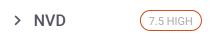
Affected versions of this package are vulnerable to Denial of Service (DoS) when trying to encode using an encoder with zero channels, or a non-initialized buffer. This leads to a hard crash.

### PoC

// Zero channels:







# 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

// Non-initialized buffer:

```
const { OpusEncoder } =
require('@discordjs/opus'); const encoder = new
OpusEncoder(48000, 2); try { const encoded =
encoder.encode(null); } catch(e) { // never
executed because of the hard crash
```

### 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, commonsfileupload:commons-fileupload.
- Crash An attacker sending crafted requests that could cause the system to crash. For Example, npm ws package

#### References

- Github Commit
- GitHub Issues
- Github PR
- Vulnerable Code

Test your applications



### Snyk Learn

Learn about Denial of Service (DoS) vulnerabilities in an interactive lesson.

Start learning

SnykSNYK-JS-**DISCORDJSOPUS-**2403100

Published 16 Jun 2022

Disclosed 16 Feb 2022

CreditCristian-Alexandru Staicu

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
-AQs
COMPANY
About
Jobs
Contact
Policies
Do Not Sell My Personal Information
CONTACT US
Support
Report a new vuln
Press Kit
Events

PRODUCT

Snyk Code

Snyk Open Source

FIND US ONLINE

TRACK OUR DEVELOPMENT







### © 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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