Denial of Service (DoS)

Affecting pg-native package, versions **<3.0.1**

INTRODUCED: 3 FEB 2022 CVE-2022-25852
CWE-400 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `pg-native` to version 3.0.1 or higher.

Overview

pg-native is a high performance native bindings between node.js and PostgreSQL via libpq with a simple API.

Affected versions of this package are vulnerable to Denial of Service (DoS) when the addons attempt to cast the second argument to an array and fail. This happens for every non-array argument passed.

Note: `pg-native` is a mere binding to npm's `libpq` library, which in turn has the addons and bindings to the actual C `libpq` library. This means that problems found in `libpq` may transitively impact npm's `pg-native`.

PoC

```
//pg-native -> poc.js let Client = require('pg-native') let client = new Client(); client.connectSync(); client.query('some str', 1, function() {}); //libpq -> poc.js var Libpq =
```

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.

```
require('libpq') const pq = new Libpq();
pq.sendQueryParams("some str", 1)
```

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 Issues
- Github PR

Snyk ID	SNYK-JS-PGNATIVE-2392365
Published	14 Jun 2022
Disclosed	3 Feb 2022
Credit	Cristian-Alexandru Staicu, Snyk Security Labs

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

DevSecCon

Join the >> community

Registered in England and Wales. Company number: 09677925

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