Command Injection

Affecting heroku-addonpool package, versions **<0.1.16**

INTRODUCED: 4 APR 2020 CVE-2020-7634 CWE-74 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `heroku-addonpool` to version 0.1.16 or higher.

Overview

heroku-addonpool is a tool that Managing Addon Pool of an App in Heroku.

Affected versions of this package are vulnerable to Command Injection. The second parameter of the exported function `HerokuAddonPool(id, app, opt)` can be controlled by users without any sanitization.

PoC

```
var Root = require("heroku-addonpool"); var root = Root("sss","& touch JHU",{}); root.setup();
```

References

- GitHub Commit

MEDIUM

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Confidentiality	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-HEROKUADDONPOOL-564428
Published	4 Apr 2020
Disclosed	4 Apr 2020
Credit	JHU System Security Lab

Report a new vulnerability | Found a mistake?

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

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