MEDIUM

Search by package name or CVE

Command Injection

Affecting codecov package, versions <3.6.5

INTRODUCED: 16 FEB 2020 CVE-2020-7597 ? CWE-78 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `codecov` to version 3.6.5 or higher.

Overview

codecov is a npm package for uploading reports to Codecov.

Affected versions of this package are vulnerable to Command Injection. The value provided as part of the `gcov-root` argument is executed by the `exec` function within lib/codecov.js. This vulnerability exists due to an incomplete fix of CVE-2020-7596.

PoC by JHU System Security Lab

```
var root = require("codecov"); var args = { "options": { 'gcov-root': "& touch exploit &", 'gcov-exec': ' ', 'gcov-args': '
' } } root.handleInput.upload(args, function(){}, function(){});
```

References

- GitHub Commit

Snyk CVSS

Exploit Maturity	Proof of concept ?
Attack Complexity	Low ?
Confidentiality	HIGH ?

See more

› NVD 8.8 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.

Test your applications

Snyk ID	SNYK-JS-CODECOV-548879
Published	16 Feb 2020
Disclosed	16 Feb 2020
Credit	JHU System Security Lab

Report a new vulnerability

Found a mistake?

Registered in England and Wales. Company number: 09677925

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