

New issue

Jump to bottom

Remote Code Execution(RCE) via insecure command formatting #2

Open mohanl0l opened this issue on Oct 2, 2020 · 0 comments

mohanl0l commented on Oct 2, 2020

It fails to restrict the arbitrary commands in the user input which results in the execution of code(RCE/Information Disclosure/DoS).

aaptjs/index.js

Line 18 in f9fab0b

18 exec(cmd, (code, stdout, stderr) => {

Raised the same issue in Hackerone as well with POC:
<https://hackerone.com/reports/996483>

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant

